

501P0373 USCO

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

11036 U.S. PTO
09/808303
03/14/01


別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出願年月日
Date of Application: 2000年 3月14日

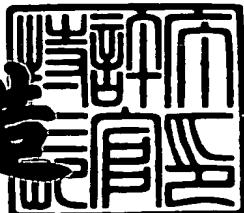
出願番号
Application Number: 特願2000-071103

出願人
Applicant(s): ソニー株式会社

2001年 1月 5日

特許庁長官
Commissioner,
Patent Office

及川耕造



出証番号 出証特2000-3109467

【書類名】 特許願
【整理番号】 00001527
【提出日】 平成12年 3月14日
【あて先】 特許庁長官殿
【国際特許分類】 G06F 17/60
【発明の名称】 コンテンツ二次配信制限システムおよびコンテンツ二次
配信制限方法、並びにプログラム提供媒体
【請求項の数】 19
【発明者】
【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内
【氏名】 石橋 義人
【特許出願人】
【識別番号】 000002185
【氏名又は名称】 ソニー株式会社
【代表者】 出井 伸之
【代理人】
【識別番号】 100101801
【弁理士】
【氏名又は名称】 山田 英治
【電話番号】 03-5541-7577
【選任した代理人】
【識別番号】 100093241
【弁理士】
【氏名又は名称】 宮田 正昭
【電話番号】 03-5541-7577
【選任した代理人】
【識別番号】 100086531
【弁理士】

【氏名又は名称】 澤田 俊夫

【電話番号】 03-5541-7577

【手数料の表示】

【予納台帳番号】 062721

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9904833

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 コンテンツ二次配信制限システムおよびコンテンツ二次配信制限方法、並びにプログラム提供媒体

【特許請求の範囲】

【請求項1】

コンテンツ受領ユーザデバイスが複数の異なるユーザデバイスに並列的にコンテンツを配信するコンテンツ二次配信におけるコンテンツ二次配信回数を制限するコンテンツ二次配信制限システムであり、

ユーザデバイス間で流通するコンテンツは、コンテンツのユーザデバイス間での販売条件を設定した販売条件情報（UCP）を持つセキュアコンテナとして構成され、

前記販売条件情報（UCP）は、ユーザデバイス間におけるコンテンツの二次配信回数の許容上限情報としてのUCP二次配信可能回数情報を含み、

前記セキュアコンテナを購入するコンテンツ受領ユーザデバイスは、コンテンツのユーザデバイス間での二次配信可能回数を格納したUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してユーザデバイス内のメモリに格納し、コンテンツのユーザデバイス間での流通時に前記UCS二次配信可能回数情報の設定条件確認処理を実行して、該条件を満足する場合にのみ、コンテンツの二次配信を実行可能とした構成を有することを特徴とするコンテンツ二次配信制限システム。

【請求項2】

コンテンツをサービスプロバイダまたは他のユーザデバイスから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）に基づいて生成する構成であることを特徴とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項3】

コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、前記セキュアコンテナ中の販売条件情報（UCP）に格納されたUCP二次配信可能回数情報中の設定回数と同一の設定回数を持つUCS二次配信可能回数情報を含む

使用制御情報（UCS）を生成してコンテンツ受領ユーザデバイスのメモリに格納する構成であることを特徴とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項4】

コンテンツをサービスプロバイダから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）に基づいて生成し、

コンテンツを他のユーザデバイスから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）および前記他のユーザデバイスに生成済みの使用制御情報（UCS）に基づいて生成する構成であることを特徴とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項5】

コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、コンテンツ提供ユーザデバイスのメモリに格納されたUCS二次配信可能回数情報中の設定回数を1つデクリメントする更新処理を実行して更新されたUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してコンテンツ受領ユーザデバイスのメモリに格納する構成であることを特徴とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項6】

前記コンテンツ二次配信制限システムにおいて、さらに、

コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、

前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録されたUCP二次配信可能回数情報と同一コンテナに基づく受領ログの発行数を比較し、UCP二次配信可能回数情報の設定を超える受領ログについては決済処理を中止する構成を有することを特徴とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項7】

前記コンテンツ二次配信制限システムにおいて、さらに、
コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信
処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理す
るサービスプロバイダまたはクリアリングセンタを有し、
前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユ
ーザデバイスから受信する前記受領ログに記録された利益配分情報に基づいて前
記コンテンツ二次配信に伴う利益配分処理の管理を行なう構成を有することを特
徴とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項8】

前記利益配分情報には、コンテンツ二次配信を実行したコンテンツ提供ユーザ
デバイスの管理者である管理ユーザが含まれ、
前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユ
ーザデバイスから受信する前記受領ログに記録された利益配分情報に基づいて、
前記コンテンツ提供ユーザデバイスの管理ユーザを含む利益配分対象者に対する
利益配分処理の管理を実行する構成であることを特徴とする請求項7に記載のコ
ンテンツ二次配信制限システム。

【請求項9】

コンテンツを提供するコンテンツ提供ユーザデバイスとコンテンツ受領ユーザ
デバイスは各々暗号処理部を有し、
ユーザデバイス間におけるデータ送信の際は、ユーザデバイス間において相互
認証処理を実行し、さらに、データ送信側が送信データに対する電子署名の生成
処理を実行して、受信側が電子署名の検証処理を実行する構成であることを特徴
とする請求項1に記載のコンテンツ二次配信制限システム。

【請求項10】

コンテンツ受領ユーザデバイスが複数の異なるユーザデバイスに並列的にコン
テンツを配信するコンテンツ二次配信におけるコンテンツ二次配信回数を制限す
るコンテンツ二次配信制限方法であり、
ユーザデバイス間で流通するコンテンツを、コンテンツのユーザデバイス間で

の販売条件を設定した販売条件情報（UCP）を持つセキュアコンテナとして構成し、

前記販売条件情報（UCP）は、ユーザデバイス間におけるコンテンツの二次配信回数の許容上限情報としてのUCP二次配信可能回数情報を含み、

前記セキュアコンテナを購入するコンテンツ受領ユーザデバイスは、コンテンツのユーザデバイス間での二次配信可能回数を格納したUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してユーザデバイス内のメモリに格納し、コンテンツのユーザデバイス間での流通時に前記UCS二次配信可能回数情報の設定条件確認処理を実行して、該条件を満足する場合にのみ、コンテンツの二次配信を実行可能としたことを特徴とするコンテンツ二次配信制限方法。

【請求項11】

コンテンツをサービスプロバイダまたは他のユーザデバイスから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）に基づいて生成することを特徴とする請求項10に記載のコンテンツ二次配信制限方法。

【請求項12】

コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、前記セキュアコンテナ中の販売条件情報（UCP）に格納されたUCP二次配信可能回数情報中の設定回数と同一の設定回数を持つUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してコンテンツ受領ユーザデバイスのメモリに格納することを特徴とする請求項10に記載のコンテンツ二次配信制限方法。

【請求項13】

コンテンツをサービスプロバイダから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）に基づいて生成し、

コンテンツを他のユーザデバイスから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）および前記他のユーザデバイスに生成済みの使用制御情報（UCS）に基づいて生成することを特徴とする請求項10に記載のコン

テンツ二次配信制限方法。

【請求項14】

コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、コンテンツ提供ユーザデバイスのメモリに格納されたUCS二次配信可能回数情報中の設定回数を1つデクリメントする更新処理を実行して更新されたUCS二次配信可能回数情報を含む使用制御情報(UCS)を生成してコンテンツ受領ユーザデバイスのメモリに格納することを特徴とする請求項10に記載のコンテンツ二次配信制限方法。

【請求項15】

前記コンテンツ二次配信制限方法において、さらに、

コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、

前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録されたUCP二次配信可能回数情報と同一コンテナに基づく受領ログの発行数を比較し、UCP二次配信可能回数情報の設定を超える受領ログについては決済処理を中止することを特徴とする請求項10に記載のコンテンツ二次配信制限方法。

【請求項16】

前記コンテンツ二次配信制限方法において、さらに、

コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、

前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録された利益分配情報に基づいて前記コンテンツ二次配信に伴う利益分配処理の管理を行なうことを特徴とする請求項10に記載のコンテンツ二次配信制限方法。

【請求項17】

前記利益分配情報には、コンテンツ二次配信を実行したコンテンツ提供ユーザ

デバイスの管理者である管理ユーザが含まれ、

前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録された利益分配情報に基づいて、前記コンテンツ提供ユーザデバイスの管理ユーザを含む利益分配対象者に対する利益分配処理の管理を実行することを特徴とする請求項16に記載のコンテンツ二次配信制限方法。

【請求項18】

コンテンツを提供するコンテンツ提供ユーザデバイスとコンテンツ受領ユーザデバイスは各々暗号処理部を有し、

ユーザデバイス間におけるデータ送信の際は、ユーザデバイス間において相互認証処理を実行し、さらに、データ送信側が送信データに対する電子署名の生成処理を実行して、受信側が電子署名の検証処理を実行することを特徴とする請求項10に記載のコンテンツ二次配信制限方法。

【請求項19】

コンテンツ受領ユーザデバイスが複数の異なるユーザデバイスに並列的にコンテンツを配信するコンテンツ二次配信におけるコンテンツ二次配信回数を制限するコンテンツ二次配信制限処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

ユーザデバイス間におけるコンテンツの二次配信回数の許容上限情報としてUCP二次配信可能回数情報を含む販売条件情報(UCP)を持つセキュアコンテナとして構成したコンテンツを購入するコンテンツ受領ユーザデバイスにおいて、コンテンツのユーザデバイス間での二次配信回数を格納したUCS二次配信可能回数情報を含む使用制御情報(UCS)を生成してユーザデバイス内のメモリに格納するステップと、

コンテンツのユーザデバイス間での流通時に前記UCS二次配信可能回数情報の設定条件確認処理を実行して、該条件を満足する場合にのみ、コンテンツの二次配信を実行可能とするステップと、

を有することを特徴とするプログラム提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明はコンテンツ二次配信制限システムおよびコンテンツ二次配信制限方法、並びにプログラム提供媒体に関する。特に、音楽、画像データ、ゲームプログラム等の各種コンテンツ情報をCD、DVD等の記録媒体を介して、あるいはネットワークを介した配信によりユーザに提供し、ユーザからコンテンツ利用に伴う利用料金の回収あるいは利用ポイントの付与等を実行するとともに、ユーザデバイスAからユーザデバイスB、ユーザデバイスC、ユーザデバイスDへのコンテンツ配信のように並列的にコンテンツを異なるユーザデバイスに対して配信するコンテンツ二次配信の回数を制限することにより、コンテンツ著作者、コンテンツ提供者等の利益を確保することを可能としたコンテンツ二次配信制限システムおよびコンテンツ二次配信制限方法に関する。

【0002】

【従来の技術】

昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータ（以下、これらをコンテンツ（Content）と呼ぶ）が、インターネット等のネットワークを介して、あるいはDVD、CD等の流通可能な記憶媒体（メディア）を介して流通している。これらの流通コンテンツは、一般にユーザの所有するPC（Personal Computer）、ゲーム機器等の記録再生機器において再生し、また付属する記録デバイス、例えばEEPROM、フラッシュメモリ等によって構成されるメモリカード、ハードディスク等に格納することが可能である。

【0003】

DVD、CD等の流通可能な記憶媒体（メディア）、あるいはメモリカード等の記憶手段に記憶されたデータ、あるいはプログラム等の様々なコンテンツは、再生機器として利用されるゲーム機器、PC等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により各記憶手段から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて

再生される。

【0004】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、コンテンツの配布時、すなわちコンテンツがネットワークを介して、あるいはDV D, CD等の記憶媒体によって流通する場合には、コンテンツの提供時に代金を回収したり、インターネット等のネットワークを介してコンテンツを配信する場合、コンテンツ配信に際してユーザのクレジット番号等のユーザ情報を取得してユーザからコンテンツ提供に対する対価、すなわち利用料金を取得する構成を採用している。

【0005】

これらのコンテンツの配布に際しては、コンテンツの許可のない複製等が行われないよう、セキュリティを考慮した構成をとるのが一般的となっており、DV D, CD等の記憶媒体（メディア）、あるいはネットワークを介したコンテンツデータの配信においては、配布コンテンツを正規なユーザに対してのみ提供する構成が各種提案されている。

【0006】

コンテンツ利用を正規ユーザにのみ提供する概念の1つに「超流通」という考えが提案されている。「超流通」は、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウェアデータであるコンテンツの提供者、あるいはコンテンツ管理者の権利保護を確保して、コンテンツを流通させるための構成である。この「超流通」の構成を図1に示す。

【0007】

コンテンツプロバイダ101、コンテンツプロバイダ102は、それぞれコンテンツ103, 104をユーザ端末105に提供する。コンテンツ103, 104には、コンテンツ固有の識別子であるコンテンツIDが付加されている。ユーザ端末105では、コンテンツIDの付加されたコンテンツを受領すると、判定処理部107において、ユーザ端末105が、そのコンテンツの利用可能な正規ユーザ端末であるか否かを判定する。この判定処理は、記憶部1, 106に記憶

されたユーザ端末のユーザIDとコンテンツ利用条件に基づいて判定される。コンテンツ利用条件は、ユーザ毎にコンテンツプロバイダが予め設定したコンテンツの利用条件である。設定したコンテンツ利用条件に応じてコンテンツの利用可と判定されると、そのコンテンツの利用履歴を記憶部2, 108にユーザIDとコンテンツIDを対応させて記憶する。

【0008】

コンテンツプロバイダ101, 102は、ユーザ端末105の記憶部2, 108に記憶されたコンテンツ利用履歴を回収して、その履歴に従ってコンテンツ利用料金をユーザに請求することができる。このように「超流通」は、ユーザ毎にコンテンツの利用条件を判定し、かつコンテンツ毎に利用履歴を記録する構成により、コンテンツの利用を正規ユーザに限定し、利用料金の回収を可能にする構成である。

【0009】

しかしながら、上記の「超流通」の構成はコンテンツの利用履歴を記録する構成を開示しているものの、利用履歴に基づく料金徴収システムについては明確に示すものではなく、料金の支払い手法は従来から提案されている方法を採用することになる。例えば（1）クレジットカード番号をユーザ端末から入力してコンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツの利用権を管理するコンテンツ利用権販売センタに送信する。（2）ユーザの銀行口座番号を端末から入力してコンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツ利用権販売センタに送信する。（3）予めコンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツ利用権販売センタにユーザ登録を行ない、クレジットカード番号、あるいは銀行口座番号を登録し、コンテンツプロバイダまたはサービスプロバイダ、あるいはコンテンツ利用権販売センタが登録済みデータに基づいて料金引き落としを実行する。これらのいずれかの方法を実行することが必要となる。

【0010】

上述の（1）～（3）の支払方法においてはユーザのクレジットカード番号、あるいは銀行口座番号が要求されることになる。従って、これらのクレジットカ

ード、銀行口座を持たない者にとっては、この支払い手続きが困難になる。さらに、昨今では、取り引きコンテンツ単位が小口化し、例えば音楽コンテンツの配信において曲目1曲のみを取り引きコンテンツとすることもある。このような場合、コンテンツの代金は、100円単位、1000円単位の小額のものとなり、これらの支払いにおいて、逐一、クレジットカード番号、あるいは銀行口座番号が要求されるという取り引き形態がコンテンツの流通を妨げる一因ともなっている。

【0011】

さらに、一旦市場に流通したコンテンツは、さらにユーザ間において取り引き、譲渡され得る。このようなユーザ間での取り引きを管理することは困難であり、不正なコピーの流通が氾濫することになる。また、ユーザ間の取り引きにおいては、一般にコンテンツを提供したユーザに対して何ら保証されないのが一般的であった。

【0012】

【発明が解決しようとする課題】

本発明は、これらの状況に鑑みてなされたものであり、ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツ利用権の販売において、クレジットカード番号、あるいは銀行口座番号を利用せず、簡易な方法、構成を構築するとともに、ユーザ間でのコンテンツの二次配布を管理するものであり、ユーザデバイスAからユーザデバイスB、ユーザデバイスC、ユーザデバイスDへのコンテンツ配信のように並列的にコンテンツを異なるユーザデバイスに対して配信するコンテンツ二次配信の回数を制限することにより、コンテンツ著作者、コンテンツ提供者等の利益を確保することを可能としたコンテンツ二次配信制限システムおよびコンテンツ二次配信制限方法を提供することを目的とする。

【0013】

【課題を解決するための手段】

本発明の第1の側面は、

コンテンツ受領ユーザデバイスが複数の異なるユーザデバイスに並列的にコン

コンテンツを配信するコンテンツ二次配信におけるコンテンツ二次配信回数を制限するコンテンツ二次配信制限システムであり、

ユーザデバイス間で流通するコンテンツは、コンテンツのユーザデバイス間での販売条件を設定した販売条件情報（UCP）を持つセキュアコンテナとして構成され、

前記販売条件情報（UCP）は、ユーザデバイス間におけるコンテンツの二次配信回数の許容上限情報としてのUCP二次配信可能回数情報を含み、

前記セキュアコンテナを購入するコンテンツ受領ユーザデバイスは、コンテンツのユーザデバイス間での二次配信可能回数を格納したUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してユーザデバイス内のメモリに格納し、コンテンツのユーザデバイス間での流通時に前記UCS二次配信可能回数情報の設定条件確認処理を実行して、該条件を満足する場合にのみ、コンテンツの二次配信を実行可能とした構成を有することを特徴とするコンテンツ二次配信制限システムにある。

【0014】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コンテンツをサービスプロバイダまたは他のユーザデバイスから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）に基づいて生成する構成であることを特徴とする。

【0015】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、前記セキュアコンテナ中の販売条件情報（UCP）に格納されたUCP二次配信可能回数情報中の設定回数と同一の設定回数を持つUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してコンテンツ受領ユーザデバイスのメモリに格納する構成であることを特徴とする。

【0016】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コ

ンテンツをサービスプロバイダから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）に基づいて生成し、コンテンツを他のユーザデバイスから受領するユーザデバイスは、前記UCS二次配信可能回数情報を含む使用制御情報（UCS）を、前記セキュアコンテナ中の販売条件情報（UCP）および前記他のユーザデバイスに生成済みの使用制御情報（UCS）に基づいて生成する構成であることを特徴とする。

【0017】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、コンテンツ提供ユーザデバイスのメモリに格納されたUCS二次配信可能回数情報中の設定回数を1つデクリメントする更新処理を実行して更新されたUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してコンテンツ受領ユーザデバイスのメモリに格納する構成であることを特徴とする。

【0018】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録されたUCP二次配信可能回数情報と同一コンテナに基づく受領ログの発行数を比較し、UCP二次配信可能回数情報の設定を超える受領ログについては決済処理を中止する構成を有することを特徴とする。

【0019】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前

記受領ログに記録された利益配分情報に基づいて前記コンテンツ二次配信に伴う利益配分処理を行なう構成を有することを特徴とする。

【0020】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、前記利益配分情報には、コンテンツ二次配信を実行したコンテンツ提供ユーザデバイスの管理者である管理ユーザが含まれ、前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録された利益配分情報に基づいて、前記コンテンツ提供ユーザデバイスの管理ユーザを含む利益配分対象者に対する利益配分処理の管理を実行する構成であることを特徴とする。

【0021】

さらに、本発明のコンテンツ二次配信制限システムの一実施態様において、コンテンツを提供するコンテンツ提供ユーザデバイスとコンテンツ受領ユーザデバイスは各々暗号処理部を有し、ユーザデバイス間におけるデータ送信の際は、ユーザデバイス間において相互認証処理を実行し、さらに、データ送信側が送信データに対する電子署名の生成処理を実行して、受信側が電子署名の検証処理を実行する構成であることを特徴とする。

【0022】

さらに、本発明の第2の側面は、

コンテンツ受領ユーザデバイスが複数の異なるユーザデバイスに並列的にコンテンツを配信するコンテンツ二次配信におけるコンテンツ二次配信回数を制限するコンテンツ二次配信制限方法であり、

ユーザデバイス間で流通するコンテンツを、コンテンツのユーザデバイス間での販売条件を設定した販売条件情報（UCP）を持つセキュアコンテナとして構成し、

前記販売条件情報（UCP）は、ユーザデバイス間におけるコンテンツの二次配信回数の許容上限情報としてのUCP二次配信可能回数情報を含み、

前記セキュアコンテナを購入するコンテンツ受領ユーザデバイスは、コンテンツのユーザデバイス間での二次配信可能回数を格納したUCS二次配信可能回数

情報を含む使用制御情報（U C S）を生成してユーザデバイス内のメモリに格納し、コンテンツのユーザデバイス間での流通時に前記U C S二次配信可能回数情報の設定条件確認処理を実行して、該条件を満足する場合にのみ、コンテンツの二次配信を実行可能としたことを特徴とするコンテンツ二次配信制限方法にある。

【0023】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、コンテンツをサービスプロバイダまたは他のユーザデバイスから受領するユーザデバイスは、前記U C S二次配信可能回数情報を含む使用制御情報（U C S）を、前記セキュアコンテナ中の販売条件情報（U C P）に基づいて生成することを特徴とする。

【0024】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、コンテンツ受領ユーザデバイスは、前記コンテンツ二次配信において、前記セキュアコンテナ中の販売条件情報（U C P）に格納されたU C P二次配信可能回数情報中の設定回数と同一の設定回数を持つU C S二次配信可能回数情報を含む使用制御情報（U C S）を生成してコンテンツ受領ユーザデバイスのメモリに格納することを特徴とする。

【0025】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、コンテンツをサービスプロバイダから受領するユーザデバイスは、前記U C S二次配信可能回数情報を含む使用制御情報（U C S）を、前記セキュアコンテナ中の販売条件情報（U C P）に基づいて生成し、コンテンツを他のユーザデバイスから受領するユーザデバイスは、前記U C S二次配信可能回数情報を含む使用制御情報（U C S）を、前記セキュアコンテナ中の販売条件情報（U C P）および前記他のユーザデバイスに生成済みの使用制御情報（U C S）に基づいて生成することを特徴とする。

【0026】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、コンテ

ンツ受領ユーザデバイスは、前記コンテンツ二次配信において、コンテンツ提供ユーザデバイスのメモリに格納されたUCS二次配信可能回数情報中の設定回数を1つデクリメントする更新処理を実行して更新されたUCS二次配信可能回数情報を含む使用制御情報(UCS)を生成してコンテンツ受領ユーザデバイスのメモリに格納することを特徴とする。

【0027】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、さらに、コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録されたUCP二次配信可能回数情報と同一コネクタに基づく受領ログの発行数を比較し、UCP二次配信可能回数情報の設定を超える受領ログについては決済処理を中止することを特徴とする。

【0028】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、コンテンツ提供ユーザデバイスから直接または間接的にコンテンツの二次配信処理に伴う受領ログを受け取り該コンテンツ二次配信に応じた決済処理を管理するサービスプロバイダまたはクリアリングセンタを有し、前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録された利益配分情報に基づいて前記コンテンツ二次配信に伴う利益配分処理の管理を行なうことを特徴とする。

【0029】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、前記利益配分情報には、コンテンツ二次配信を実行したコンテンツ提供ユーザデバイスの管理者である管理ユーザが含まれ、前記サービスプロバイダまたはクリアリングセンタは、前記コンテンツ提供ユーザデバイスから受信する前記受領ログに記録された利益配分情報に基づいて、前記コンテンツ提供ユーザデバイスの管理ユーザを含む利益配分対象者に対する利益配分処理の管理を実行することを特徴と

する。

【0030】

さらに、本発明のコンテンツ二次配信制限方法の一実施態様において、コンテンツを提供するコンテンツ提供ユーザデバイスとコンテンツ受領ユーザデバイスは各々暗号処理部を有し、ユーザデバイス間におけるデータ送信の際は、ユーザデバイス間において相互認証処理を実行し、さらに、データ送信側が送信データに対する電子署名の生成処理を実行して、受信側が電子署名の検証処理を実行することを特徴とする。

【0031】

さらに、本発明の第3の側面は、

コンテンツ受領ユーザデバイスが複数の異なるユーザデバイスに並列的にコンテンツを配信するコンテンツ二次配信におけるコンテンツ二次配信回数を制限するコンテンツ二次配信制限処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、

ユーザデバイス間におけるコンテンツの二次配信回数の許容上限情報としてUCP二次配信可能回数情報を含む販売条件情報(UCP)を持つセキュアコンテナとして構成したコンテンツを購入するコンテンツ受領ユーザデバイスにおいて、コンテンツのユーザデバイス間での二次配信回数を格納したUCS二次配信可能回数情報を含む使用制御情報(UCS)を生成してユーザデバイス内のメモリに格納するステップと、

コンテンツのユーザデバイス間での流通時に前記UCS二次配信可能回数情報の設定条件確認処理を実行して、該条件を満足する場合にのみ、コンテンツの二次配信を実行可能とするステップと、

を有することを特徴とするプログラム提供媒体にある。

【0032】

本発明の第3の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、CDやFD

、MO、DVDなどの記憶媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【0033】

このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【0034】

【発明の実施の形態】

以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。

【0035】

【実施例】

【1. システム概要】

まず、本発明のコンテンツ取り引きシステムの概要について図2を用いて説明する。図2には、情報、すなわち音楽データ、画像データ、ゲーム等の各種プログラム等のコンテンツを利用するユーザデバイス220、ユーザデバイス220に対してコンテンツを提供するサービスプロバイダ240、コンテンツ利用に係る電子マネーの決済処理を実行するクリアリングセンタ260と、コンテンツ利用に伴う現実のお金の流れを処理する例えば銀行等の金融機関である口座管理機関280が示されている。

【0036】

なお、図2に示すコンテンツ取り引きシステム構成は一例であり、図2に示す構成以外にも、様々なコンテンツ取り引きシステムが構成され得る。例えばサービスプロバイダ240を、実際にコンテンツを作成するコンテンツ提供プロバイダと、コンテンツ提供プロバイダからコンテンツを受領し実際のユーザに配布す

るコンテンツの流通サービスを提供するサービスプロバイダ等からなる複数構成としてもよい。また、クリアリングセンタ260と、口座管理機関280とを1つの機関とした構成であってもよい。さらに、図2では、ユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260、口座管理機関280がそれぞれ1つのみ示されているが、実際にはそれぞれの構成が複数存在することが可能である。また、後段で詳細に説明するが、本発明のコンテンツ取り引きシステムでは、複数の異なるユーザデバイス間でのコンテンツ取り引きを可能とした構成を持つ。

【0037】

図2において、コンテンツを利用するユーザデバイス220は、コンテンツの利用料金を電子マネー221を用いて支払う。電子マネー221に対する入金処理は、ユーザデバイス220を管理する管理ユーザが、必要に応じて銀行等の金融機関である口座管理機関280に現金を預けたユーザ口座281を開設し、ユーザ口座281からクリアリングセンタ管理下のユーザ電子マネー口座283へ振り込みを行ない、ユーザの振り込んだ金額を上限として、ユーザの電子マネー221に使用可能金額（電子マネー残高）が設定され、振り込みを確認した口座管理機関280は電子マネーの決済処理、残高管理等を行なうクリアリングセンタ260に、ユーザの振込金額（電子マネーの設定金額）を通知して、電子マネーとして利用可能な金額をクリアリングセンタ260が管理する。

【0038】

クリアリングセンタ260は、ユーザデバイス220の管理ユーザの使用可能な金額、ユーザの使用するユーザデバイス220の識別子等をデータとして持つ電子マネー発行ログをユーザデバイス220に送信し、ユーザデバイス220は、発行ログ251をユーザデバイス220内に格納する。発行ログ251については、後段で詳細に説明する。

【0039】

ユーザデバイス220は、音楽データ、画像データ、ゲーム等の各種プログラム等のコンテンツをサービスプロバイダ240から提供を受ける際、電子マネー221を用いてサービスプロバイダ240にコンテンツの利用料金の支払いを行

なう。この際、電子マネー221の残高から利用料金を減額する。また、ユーザデバイス220は、発行ログ情報と、コンテンツの利用金額、コンテンツの利用料金の受け取り先情報等を記録したデータからなる利用情報をデータとして持つ利用ログ252をサービスプロバイダ240に送信する。

【0040】

サービスプロバイダ240は、ユーザデバイス220から受領した利用ログ252の検証処理を実行して、利用ログ252に基づいて、コンテンツ利用料金の支払元、受領日時等からなる受領情報を持つ受領ログ253を生成してクリアリングセンタ260に送信する。この際、クリアリングセンタ260は、決済処理に関する実際の現金の受け渡し情報（配分情報）を口座管理機関280に振替要求として送信し、口座管理機関280は、クリアリングセンタ260からの振替要求に基づいて、サービスプロバイダ口座282、クリアリングセンタ283相互間において、金額振替を実行する。

【0041】

なお、図2では、説明の複雑化をさけるためにユーザデバイス220の管理ユーザのユーザ口座281、サービスプロバイダ口座282、クリアリングセンタ283のみが示されているが、口座管理機関280は、コンテンツ作成者の口座、あるいは、コンテンツの販売店舗等の口座等を持ち、それぞれに予め定められた設定に従って振替を行なう構成としてもよい。これらの料金振替設定情報をコンテンツと共に流通させる形態については、後段で説明する。

【0042】

【2. ユーザデバイス】

図3に本発明のコンテンツ取り引きシステムに使用されるユーザデバイスの一実施例に係る構成ブロック図を示す。ユーザデバイス300は、コンテンツを格納する記録デバイス350を持つ。

【0043】

ユーザデバイス300は、例えばパーソナル・コンピュータ（PC：Personal Computer）、あるいはゲーム機器等によって構成される。ユーザデバイス300は、ユーザデバイス300における暗号処理時の記録デバイス350との通信

制御を含む統括的制御を実行する制御部301、暗号処理全般を司る記録再生器暗号処理部302、記録再生器に接続される記録デバイス350と認証処理を実行しデータの読み書きを行う記録デバイスコントローラ303、DVDなどのメディア360から少なくともデータの読み出しを行う読み取り部304、外部とデータの送受信を行う通信部305を有する。

【0044】

ユーザデバイス300は、制御部301の制御により記録デバイス350に対するコンテンツデータのダウンロード、記録デバイス350からのコンテンツデータ再生を実行する。記録デバイス350は、ユーザデバイス300に対して好ましくは着脱可能な記憶媒体、例えばメモリカード等であり、EEPROM、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきRAMなどによって構成される外部メモリ352を有する。

【0045】

ユーザデバイス300は、図3の左端に示す記憶媒体、DVD、CD、FD、HDDに格納されたコンテンツデータを入力可能なインターフェースとしての読み取り部304、インターネット等のネットワークから配信されるコンテンツデータを入力可能なインターフェースとしての通信部305を有し、外部からコンテンツを入力する。

【0046】

ユーザデバイス300は、電子マネー310をデバイスに固定、あるいは着脱可能に有しており、利用情報、残高金額等をフラッシュメモリ、EEPROM等で構成されるメモリ313に記憶する。電子マネー310が外部と通信するデータは、電子マネーを所有する個人ID、利用金額等であり、これらが暗号化されて電子マネー310に入出力する。これらのデータの暗号処理を実行するのが暗号処理部312でありデータ入出力制御、暗号処理部での処理制御を制御部311が実行する。電子マネー310は、例えばセキュリティ用ICカードのようなSAM：Secure Application Moduleとして構成される。

【0047】

さらに、ユーザデバイス300は、SAMにより構成された暗号処理部302を有する。なお、図3の例では、暗号処理部302のSAMと電子マネー310のSAMとが別構成として示されているが、これらのSAMは1つのモジュールとして構成してもよい。暗号処理部302は、読み取り部304または通信部305を介して外部から入力されるコンテンツデータを記録デバイス350にダウンロード処理する際、あるいはコンテンツデータを記録デバイス350から再生、実行する際の認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する。さらに、コンテンツの利用料金の支払い情報として発行ログの受領、利用ログの生成処理、送信処理等の際の認証処理、暗号処理、データの検証処理等を実行する。暗号処理部302は、暗号処理部302全体を制御する制御部306、暗号処理用の鍵などの情報を保持し、外部から容易にデータを読み出せないように処理が施された内部メモリ307、暗号化処理、復号化処理、認証用のデータの生成・検証、乱数の発生などを行う暗号／復号化部308から構成されている。

【0048】

暗号処理部302、電子マネー310部は、SAM : Secure Application Moduleによって構成することで、不正なデータの書き換えを防止することができる。暗号処理部302、電子マネー310部には、セキュリティの高い情報として、ユーザデバイス300の識別子（ID）、電子マネーの残高、後述する電子マネー発行ログ、さらに、認証処理、暗号処理等に用いる各種の鍵情報が格納される。なお、後段で説明するが、電子マネー発行ログには電子マネーによる利用可能な金額に相当する発行金額が記録されユーザデバイスに格納される。

【0049】

制御部301は、例えば、ユーザデバイス300と通信部305を介して通信手段に接続されたサービスプロバイダと暗号処理部302との相互認証処理の仲介処理、セッション鍵で暗号化されて送付されるコンテンツ鍵の暗号処理部302における復号処理における仲介制御、さらに記録デバイス350が装着された際に記録デバイスコントローラ303を介して記録デバイス350に初期化命令を送信したり、あるいは、暗号処理部302の暗号／復号化部308と記録デバ

イス暗号処理部351間で行われる相互認証処理、署名検証処理、暗号化、復号化処理等、各種処理における仲介処理を行なう。

【0050】

暗号処理制御部306は、ユーザデバイス300において実行される認証処理、暗号化／復号化処理等の暗号処理全般に関する制御を実行する制御部であり、例えば、サービスプロバイダとの相互認証処理の制御、ユーザデバイス300と記録デバイス350との間で実行される認証処理の制御、暗号処理部302の暗号／復号化部308において実行される各種処理、例えばコンテンツ鍵（コンテンツ暗号化鍵）の鍵交換処理、ダウンロード、あるいは再生コンテンツデータに関する暗号処理の実行命令等、暗号処理全般に関する制御を行なう。

【0051】

内部メモリ307は、ユーザデバイス300において実行される相互認証処理、暗号化、復号化処理等、各種処理において必要となる鍵データ、あるいは記録再生器の識別データ等を格納する。記録再生器の識別データは、例えばサービスプロバイダとの相互認証処理等において用いられる。

【0052】

暗号／復号化部308は、内部メモリ307に格納された鍵データ等を使用して、外部から入力されるコンテンツデータおよび電子マネーを使用した利用金支払い処理に伴うデータ転送時の認証処理、暗号化処理、復号化処理、データの検証、乱数の発生などの処理を実行する。

【0053】

暗号処理部302の内部メモリ307は、暗号鍵などの重要な情報を持しているため、外部から不正に読み出しにくい構造にしておく必要がある。従って、暗号処理部302は、外部からアクセスしにくい構造を持った半導体チップで構成され、多層構造を有し、その内部のメモリはアルミニウム層等のダミー層に挟まれるか、最下層に構成され、また、動作する電圧または／かつ周波数の幅が狭い等、外部から不正にデータの読み出しが難しい特性を有する耐タンパメモリとして構成される。

【0054】

ユーザデバイス300は、これらの暗号処理機能の他に、中央演算処理装置（メインCPU：Central Processing Unit）321、RAM（Random Access Memory）322、ROM（Read Only Memory）323、AV処理部325、入力インターフェース324、PIO（パラレルI/Oインターフェース）326、SIO（シリアルI/Oインターフェース）327を備えている。

【0055】

中央演算処理装置（メインCPU：Central Processing Unit）321、RAM（Random Access Memory）322、ROM（Read Only Memory）323は、ユーザデバイス300本体の制御系として機能する構成部であり、主として暗号処理部302で復号されたデータの再生を実行する再生処理部として機能する。例えば中央演算処理装置（メインCPU：Central Processing Unit）321は、制御部301の制御のもとに記録デバイスから読み出されて復号されたコンテンツデータをAV処理部325へ出力する等、コンテンツの再生、実行に関する制御を行なう。

【0056】

RAM322は、CPU321における各種処理用の主記憶メモリとして使用され、メインCPU321による処理のための作業領域として使用される。ROM323は、メインCPU321で起動されるOS等を立ち上げるための基本プログラム等が格納される。

【0057】

AV処理部325は、具体的には、例えばMPEG2デコーダ、ATRACデコーダ、MP3デコーダ等のデータ圧縮伸長処理機構を有し、記録再生器本体に付属または接続された図示しないディスプレイまたはスピーカ等のデータ出力機器に対するデータ出力のための処理を実行する。

【0058】

入力インターフェース324は、接続されたコントローラ、キーボード、マウス等、各種の入力手段からの入力データをメインCPU321に出力する。メインCPU321は、例えば実行中のゲームプログラム等に基づいて使用者からのコントローラからの指示に従った処理を実行する。

【0059】

PIO(パラレルI/Oインターフェース)326、SIO(シリアルI/Oインターフェース)327は、メモリカード、ゲームカートリッジ等の記憶装置、携帯用電子機器等との接続インターフェースとして使用される。

【0060】

記録デバイス350は、例えばユーザデバイス300に対して着脱可能な記憶媒体であり、例えばメモリカードによって構成される。記録デバイス350は暗号処理部351、外部メモリ352を有する。

【0061】

記録デバイス暗号処理部351は、ユーザデバイス300からのコンテンツデータのダウンロード、または記録デバイス350からユーザデバイス300へのコンテンツデータの再生処理時等におけるユーザデバイス300と記録デバイス350間の相互認証処理、暗号化処理、復号化処理、さらにデータの検証処理等を実行する処理部であり、ユーザデバイス300の暗号処理部と同様、制御部、内部メモリ、暗号／復号化部等を有する。外部メモリ352は、前述したように、例えばEEPROM、フラッシュメモリ等の不揮発メモリ、ハードディスク、電池つきRAMなどによって構成されコンテンツデータの格納、コンテンツ鍵の格納等に使用される。

【0062】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウェア・コンテンツを提供するサービスプロバイダは、提供コンテンツを暗号化して、CD、DVD等のメディア、あるいはネットワークを介してユーザに提供する。コンテンツの利用料金は、ネットワーク等の通信手段を介して電子マネーにより支払われる。

【0063】

[3. コンテンツ取り引きシステムにおける決済処理]

(3-1) 概要

図4は、本発明のコンテンツ取り引きシステムにおけるユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260と、口座管理機関28

0において実行されるコンテンツ利用料金の決済に伴うデータ転送を説明する図である。

【0064】

本発明のコンテンツ取り引きシステムにおけるユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260と、口座管理機関280相互間で実行されるデータ転送は、基本的に通信内容の漏洩を防止するために通信データの暗号化処理を施して実行する。また、データ送信に先立ち、通信相互間において相互認証処理が実行されて認証が成立した場合にのみ、例えば電子マネーによる支払いデータ等を暗号化データとして送信する。認証処理については後段で説明する。

【0065】

図4に示す公開鍵証明書発行局（IA：Issuer Authority）410は、ユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260と、口座管理機関280相互で行われる暗号文書の通信に用いられる各々の公開鍵を証明するための第三者機関であり、各々の公開鍵の証明書を発行する認証局としての役割を有する。

【0066】

ユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260、口座管理機関280は、図4に示すように、それぞれ、公開鍵証明書発行局（IA）410の公開鍵を有する。さらに、ユーザデバイス220は、ユーザデバイス固有の公開鍵情報を記録したユーザデバイス証明書、さらにユーザデバイス220を使用するユーザ固有の公開鍵情報を記録したユーザ証明書を公開鍵証明書発行局410から受領し格納している。

【0067】

公開鍵証明書は、公開鍵暗号方式における暗号処理の信頼性を維持するためのものである。公開鍵証明書は、例えばユーザデバイスであればユーザデバイスIDと公開鍵等を公開鍵証明書発行局（IA）410に提出することにより、公開鍵証明書発行局（IA）410が公開鍵証明書発行局（IA）のIDや有効期限等の情報を付加し、さらに公開鍵証明書発行局（IA）による署名を付加して作

成する証明書である。または、サービスを提供するサービスプロバイダが保持する登録局（（RA）：Registration Authority）にユーザデバイスIDと公開鍵を提出し、登録を申請し、登録局（RA）が公開鍵証明書発行局（IA）に対しで発行依頼を行なってユーザデバイスに公開鍵証明書を送付する構成としてもよい。

【0068】

図5に公開鍵証明書の例を示す。図5に示すように公開鍵証明書には、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、公開鍵証明書発行局（IA）の名前、証明書の有効期限、証明書利用者の名前（ユーザID）、証明書利用者の公開鍵並びに電子署名を含む。

【0069】

電子署名は、証明書のバージョン番号、公開鍵証明書発行局（IA）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、公開鍵証明書発行局（IA）の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して公開鍵証明書発行局（IA）の秘密鍵を用いて生成したデータである。

【0070】

公開鍵証明書発行局（IA）410は、図5に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（リボケーション：Revocationと呼ぶ）を行う。また、必要に応じて公開鍵・秘密鍵の生成も行う。

【0071】

一方、この公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（IA）の公開鍵（IA公開鍵）を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者、すなわち図4では、ユーザデバイス220、サービスプロバイダ240、クリアリン

グセンタ260、口座管理機関280は、共通の公開鍵証明書発行局（IA）の公開鍵を保持している必要がある。

【0072】

図4に示すように、ユーザデバイス220は、IA公開鍵と、ユーザデバイス証明書、ユーザ証明書を有し、サービスプロバイダ240は、IA公開鍵と、サービスプロバイダ証明書、クリアリングセンタ260は、IA公開鍵と、クリアリングセンタ証明書、口座管理機関280は、IA公開鍵と、口座管理機関証明書とを有している。これらユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260、口座管理機関280の相互間においては、各証明書を用いた公開鍵暗号方式、あるいは共通鍵暗号方式を用いた通信を実行して、コンテンツ利用料金の支払い、決済処理用のデータを転送する。なお、口座管理機関280への通信は既存のSSL(Secure Socket Layer)等を用いた通信としてもよい。

【0073】

(3-2) コンテンツ料金処理において使用される各種ログ

本発明のコンテンツ取り引きシステムにおいては、コンテンツの利用料金の決済処理のための情報、具体的には、コンテンツ利用に関する各種の取り引き情報を記録した各種のログ情報が図2で説明したユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260間で転送される。すなわちユーザデバイス220が有する発行ログ251、ユーザデバイス220がコンテンツ利用料金支払い時に生成してサービスプロバイダ240に送信する利用ログ252、サービスプロバイダ240が利用ログ252に基づいて生成してクリアリングセンタ260に送信する受領ログ253である。ここでは、これらの各ログについて図6を用いて説明する。

【0074】

ユーザデバイス220の有する発行ログは、図2に示すクリアリングセンタ260が発行した電子マネー情報であり、発行ログに記録された情報に対して発行ログの発行者（例えばクリアリングセンタ）の署名（電子署名）がなされ、発行ログの記録データの改竄が防止されている。発行ログには、図6に示すように、

電子マネーにおいて利用可能な総金額に相当する発行金額、ユーザデバイスまたは利用者の識別子であるユーザデバイスIDまたはユーザID、有効期限、発行ログの発行者(例えばクリアリングセンタ)が管理するシリアル番号が記録されている。

【0075】

発行ログは、利用者の要求に基づいて発行者(クリアリングセンタ)が発行する。例えばユーザがクリアリングセンタ260の管理口座のある銀行に出向き、クリアリングセンタの管理口座に利用希望額を振り込んだり、あるいはクレジットカードを使用して振り込みを行なうことで実際の金額移動を行なう。クリアリングセンタ260は、銀行から振り込み情報を受け取って振り込みの確認を行ない、振り込み金額に対応する金額を発行ログの発行金額として設定する。あるいは、ユーザから直接クリアリングセンタ260に発行ログの発行要求と、ユーザの銀行口座からクリアリングセンタ260の管理口座への振替依頼を行なって、クリアリングセンタ260が銀行に対して振り替え要求を行なって、振替金額に応じた発行金額を設定した発行ログを発行する構成としてもよい。

【0076】

ユーザデバイス220は、クリアリングセンタ260の発行した発行ログに設定された発行金額を限度として、コンテンツの利用料金を電子マネー221を用いて支払う。電子マネー221による支払い処理の際には、SAMによって構成される電子マネー221に記録されている電子マネー残高がチェックされ、残高が支払い金額より少ない場合は、電子マネー221による支払いは実行できない。残高が支払い金額以上である場合にのみ電子マネーによる支払いが実行される。電子マネー221に記録されている発行ログに基づく電子マネー使用可能残高は、支払処理により更新される。

【0077】

発行ログに設定された発行金額に相当する金額を使いきった場合、すなわち発行ログに基づく電子マネー使用可能残高が0になったユーザは、所定の金額をクリアリングセンタ管理口座に振り込んで新たな発行ログの発行をクリアリングセンタに要求することができる。また、残高が0にならない場合であっても、ユー

ザは新たな発行ログの追加発行をクリアリングセンタ260に要求することができる。

【0078】

クリアリングセンタ260による発行ログの追加発行処理について説明する。まず、ユーザは追加利用する金額をクリアリングセンタ管理口座に振り込みクリアリングセンタ260に、発行ログの追加発行を要求する。クリアリングセンタ260は、発行ログの追加発行を要求してきたユーザデバイスから、すでに発行済みの「発行ログーo1d」と、電子マネー221に記録されている「発行ログーo1d」に基づく電子マネー使用可能残高データの送信を要求し、これらのデータを受領する。クリアリングセンタ260は、ユーザの振り込み金額と、ユーザから受信した「発行ログーo1d」に基づく電子マネー使用可能残高との合計を新たな発行ログである「発行ログーnew」の発行金額として設定して新たな発行ログ「発行ログーnew」をユーザデバイスに送信する。

【0079】

上述の処理において、クリアリングセンタ260は、ユーザから受信する「発行ログーo1d」に基づく電子マネー使用可能残高が、クリアリングセンタ260内のユーザ残高管理サーバの残高データと一致しない場合がある。これは、受領ログの精算処理が遅れて行われる場合があるからである。この場合、クリアリングセンタ260は、ユーザIDと発行ログシリアル番号と、各発行ログに対する残高をユーザ残高管理サーバ263において管理し、第2の発行ログの追加発行をする。例えば「発行ログーo1d」の発行金額が¥10,000で、¥8,000が利用済みで、ユーザデバイス220の電子マネーの残高データが¥2,000であるとき、クリアリングセンタ260において、¥5,000の受領ログ精算のみが処理済であるとすると、¥3,000の未処理金額があることになる。ここで、ユーザデバイス220が新たに¥20,000の発行ログの追加発行要求を行なったとする。

【0080】

この時点において、クリアリングセンタ260が発行金額の¥20,000の「発行ログーnew」を発行すると、クリアリングセンタ260のユーザ残高管

理サーバ263の当該ユーザの発行ログ関連データは、【発行ログーo1d：ユーザID：残高¥5,000】と、【発行ログーnew：ユーザID：残高¥20,000】となる。その後、クリアリングセンタ260が、未回収分の¥3,000の受領ログの精算を行なった場合は、【発行ログーo1d：ユーザID：残高¥2,000】と、【発行ログーnew：ユーザID：残高¥20,000】となる。なお、いずれの発行ログに基づく受領ログであるかは、発行ログシリアル番号で区別可能である。また、クリアリングセンタ260は、ユーザから受信した「発行ログーo1d」に基づく電子マネー使用可能残高データを受信した際に未回収残高（上記の例では¥3,000）を未回収残高データとして設定して精算処理を実行するようにしてもよい。

【0081】

ユーザデバイス220は、コンテンツの利用料金を電子マネー221を用いて支払う処理を実行すると、利用ログを生成して、これをサービスプロバイダ240に送信する。利用ログには、ユーザデバイス220の有する発行ログ情報に加えて、利用情報として、コンテンツの対価として支払った金額に対応する利用金額、料金の受け取り先情報、さらに、ユーザデバイス側で管理するシリアル番号が記録されている。なおさらに、ユーザの電子マネーの現在の残高情報と利用サービス情報を付加する構成としてもよい。これらの情報に対してユーザデバイス220の署名（電子署名）がなされてユーザデバイス220からサービスプロバイダ240に送信される。ユーザデバイス220は、利用ログをサービスプロバイダ240に送信するとともに、利用ログをSAM外部の記憶手段に格納する。

【0082】

さらに、サービスプロバイダ240は、利用ログに基づいて受領ログを生成して、これを電子マネーの決済処理を行なうクリアリングセンタ260に送信する。受領ログは、図6に示すように、利用ログ情報に加えて、受領情報として、料金の支払元情報、受領日時、受領者（本例ではサービスプロバイダ）の管理するシリアル番号が記録されている。これらの情報に対して受領者（サービスプロバイダ240）の署名（電子署名）がなされてサービスプロバイダ240からクリアリングセンタ260に送信される。サービスプロバイダ240は、受領ログを

クリアリングセンタ260に送信するとともに、受領ログをSAM外部の記憶手段に格納する。

【0083】

なお、コンテンツがユーザ間で取り引きされる場合は、受領ログにはサービスプロバイダの署名ではなく、コンテンツを供給したユーザの署名がなされる。ユーザ間のコンテンツ取り引き（二次配信）については、後段で説明する。

【0084】

上記の説明および図4で示すように利用ログは、その生成者であるユーザデバイス220からサービスプロバイダ240に送信されるとともにユーザデバイス220内に格納され、受領ログは、その生成者であるサービスプロバイダ240からクリアリングセンタ260に送信されるとともに、サービスプロバイダ240内に格納される。これらのログ保存は、後日振込報告、支払報告等があった場合に、照合処理を実行可能とするためである。各ログをSAM内に保存しないのは、同一のログがクリアリングセンタ260に保管されており、万が一改竄された場合でも正しいログ情報をクリアリングセンタ260の保管ログから取り出すことが可能であるからである。

【0085】

(3-3) 電子署名

これら各ログに付加される電子署名について簡単に説明する。まず、電子署名データの生成処理方法の例の1つとして共通鍵暗号方式におけるDESを用いた例を説明する。なお、本発明においては、DES以外にも、同様の共通鍵暗号方式における処理として例えばFEAL (Fast Encipherment ALgorithm: NTT)、AES (Advanced Encryption Standard: 米国次期標準暗号) 等を用いることも可能である。

【0086】

一般的なDESを用いた電子署名の生成方法を図7を用いて説明する。まず、電子署名を生成するに先立ち、電子署名の対象となるメッセージを8バイト単位に分割する（以下、分割されたメッセージをM1、M2、…、MNとする）。そして、初期値 (Initial Value (以下、IVとする)) とM1を排他的論理

和する（その結果をI1とする）。次に、I1をDES暗号化部に入れ、鍵（以下、K1とする）を用いて暗号化する（出力をE1とする）。続けて、E1およびM2を排他的論理和し、その出力I2をDES暗号化部へ入れ、鍵K1を用いて暗号化する（出力E2）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたENが電子署名になる。この値は一般にはメッセージ認証符号（MAC（Message Authentication Code））と呼ばれ、メッセージの改竄チェックに用いられる。また、このように暗号文を連鎖させる方式のことをCBC（Cipher Block Chaining）モードと呼ぶ。このMAC値の検証時には、検証者が生成時と同様の方法でMAC値を生成し、同一の値が得られた場合、検証成功とする。

【0087】

本発明のコンテンツ取り引きシステムにおいて使用される発行ログ251、利用ログ252、受領ログ253には、図6で説明した各種情報が含まれ、これらが検証対象のメッセージに対応する。従って、これらのデータ、あるいはこれらのデータに基づいて生成されるデータを図7に示すDES暗号処理部に入力するメッセージとして電子署名を生成する。

【0088】

次に、公開鍵暗号方式を用いた電子署名の生成方法を図8を用いて説明する。図8に示す処理は、EC-DSA（Elliptic Curve Digital Signature Algorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ECCと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばRSA暗号（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【0089】

図8の各ステップについて説明する。ステップS1において、pを標数、a、bを楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、Gを楕円曲線上のベースポイント、rをGの位数、Ksを秘密鍵（ $0 < Ks < r$ ）とする。ステップS2

おいて、メッセージMのハッシュ値を計算し、 $f=Hash(M)$ とする。

【0090】

ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、MD4、MD5、SHA-1などが用いられる場合もあるし、DES-CBCが用いられる場合もある。この場合は、最終出力値となるMAC（チェック値：ICVに相当する）がハッシュ値となる。

【0091】

続けて、ステップS3で、乱数u ($0 < u < r$) を生成し、ステップS4でベースポイントをu倍した座標V (Xv, Yv) を計算する。なお、楕円曲線上の加算、2倍算は次のように定義されている。

【0092】

【数1】

$P=(X_a, Y_a), Q=(X_b, Y_b), R=(X_c, Y_c)=P+Q$ とすると、

$P \neq Q$ の時（加算）、

$$X_c = \lambda^2 - X_a - X_b$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (Y_b - Y_a) / (X_b - X_a)$$

$P=Q$ の時（2倍算）、

$$X_c = \lambda^2 - 2X_a$$

$$Y_c = \lambda \times (X_a - X_c) - Y_a$$

$$\lambda = (3(X_a)^2 + a) / (2Y_a)$$

【0093】

これらを用いて点Gのu倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。G、 $2 \times G$ 、 $4 \times G \dots$ を計算し、uを2進数展開し

て1が立っているところに対応する $2^i \times G$ (G を i 回2倍算した値 (i は u のLSBから数えた時のビット位置)) を加算する。

【0094】

ステップS5で、 $c = X v \bmod r$ を計算し、ステップS6でこの値が0になるかどうか判定し、0でなければステップS7で $d = [(f + c K s) / u] \bmod r$ を計算し、ステップS8で d が0であるかどうか判定し、 d が0でなければ、ステップS9で c および d を電子署名データとして出力する。仮に、 r を160ビット長の長さであると仮定すると、電子署名データは320ビット長となる。

【0095】

ステップS6において、 c が0であった場合、ステップS3に戻って新たな乱数を生成し直す。同様に、ステップS8で d が0であった場合も、ステップS3に戻って乱数を生成し直す。

【0096】

次に、公開鍵暗号方式を用いた電子署名の検証方法を、図9を用いて説明する。ステップS11で、 M をメッセージ、 p を標数、 a 、 b を楕円曲線の係数（楕円曲線： $y^2 = x^3 + ax + b$ ）、 G を楕円曲線上のベースポイント、 r を G の位数、 G および $Ks \times G$ を公開鍵（ $0 < Ks < r$ ）とする。ステップS12で電子署名データ c および d が $0 < c < r$ 、 $0 < d < r$ を満たすか検証する。これを満たしていた場合、ステップS13で、メッセージ M のハッシュ値を計算し、 $f = H a s h (M)$ とする。次に、ステップS14で $h = 1/d \bmod r$ を計算し、ステップS15で $h_1 = f h \bmod r$ 、 $h_2 = c h \bmod r$ を計算する。

【0097】

ステップS16において、既に計算した h_1 および h_2 を用い、点 $P = (X_p, Y_p) = h_1 \times G + h_2 \cdot Ks \times G$ を計算する。電子署名検証者は、公開鍵 G および $Ks \times G$ を知っているので、図8のステップS4と同様に楕円曲線上の点のスカラーベ倍の計算ができる。そして、ステップS17で点 P が無限遠点かどうか判定し、無限遠点でなければステップS18に進む（実際には、無限遠点の判定はステップS16できてしまう。つまり、 $P = (X, Y), Q = (X, -Y)$

) の加算を行うと、 λ が計算できず、 $P + Q$ が無限遠点であることが判明している)。ステップS18で $X_p \bmod r$ を計算し、電子署名データcと比較する。最後に、この値が一致していた場合、ステップS19に進み、電子署名が正しいと判定する。

【0098】

電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【0099】

ステップS12において、電子署名データcまたはdが、 $0 < c < r$ 、 $0 < d < r$ を満たさなかった場合、ステップS20に進む。また、ステップS17において、点Pが無限遠点であった場合もステップS20に進む。さらにまた、ステップS18において、 $X_p \bmod r$ の値が、電子署名データcと一致していなかった場合にもステップS20に進む。

【0100】

ステップS20において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【0101】

本発明のコンテンツ取り引きシステムにおいては、例えばユーザデバイス220がコンテンツの利用料金を電子マネー221を用いて支払う際に、利用ログ251を生成サービスプロバイダ240に送付する。この利用ログにはユーザデバイスの署名が付加されて、サービスプロバイダ240によって検証処理がなされる。またサービスプロバイダ240が生成してクリアリングセンタ260に送付する受領ログにはサービスプロバイダの署名が付加されて、クリアリングセンタ260によって検証処理がなされる。またクリアリングセンタ260が発行して、ユーザデバイス220に送信する発行ログにはクリアリングセンタの署名が付加されてユーザデバイス220において検証処理が実行される。

【0102】

(3-4) シリアル番号の付与方法

前述の図6の説明において、発行ログ、利用ログ、受領ログのそれぞれにはそれぞれのログ生成者、すなわち、発行ログであればクリアリングセンタ、利用ログであればユーザデバイス、受領ログであればサービスプロバイダ固有のシリアル番号が付与される。このシリアル番号の付与方法の一例を説明する。各ログ生成者は固有の秘密鍵K（例えばSAM内に保管）と、付与済みのシリアル番号N1を用いて次のシリアル番号N2を生成する。例えば $N_2 = DES(K, N_1)$ とする。最終的に各ログ情報を含む受領ログを受領するクリアリングセンタ260は、シリアル番号を付与するユーザデバイス、サービスプロバイダの秘密鍵Kをすべて管理しており、受領ログを受信した際、各ログのシリアル番号をチェックして、不正なシリアル番号の有無を検証する。不正が見つかった場合は、その受領ログに基づく精算処理を中止する。このようにシリアル番号を管理することにより、不正な金額移動を防止することが可能

【0103】

（3-5）相互認証処理およびデータ通信

図4に示すユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260、口座管理機関280の相互間におけるコンテンツ料金の支払いに関するデータ通信は、暗号化データとして送信する。例えば、図6で説明した各種ログの情報を暗号化して転送する。暗号化処理方式としては様々な態様が可能であるが、図5で説明した公開鍵証明書発行局（IA）410の発行した公開鍵証明書を用いた相互認証処理を実行して、相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が1つの好ましい方式である。

【0104】

共通鍵暗号方式を用いた相互認証方法を、図10を用いて説明する。図10において、共通鍵暗号方式としてDESを用いているが、前述のように同様な共通鍵暗号方式であればいずれでもよい。図10において、A、Bは図4におけるユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260、口座管理機関280の通信を実行する2つの構成要素に対応する。

【0105】

まず、Bが64ビットの乱数R_bを生成し、R_bおよび自己のIDであるID(b)をAに送信する。これを受信したAは、新たに64ビットの乱数R_aを生成し、R_a、R_b、ID(b)の順に、DESのCBCモードで鍵K_{a b}を用いてデータを暗号化し、Bに返送する。図7に示すDESのCBCモード処理構成によれば、R_aがM1、R_bがM2、ID(b)がM3に相当し、初期値：IV = 0としたときの出力E₁、E₂、E₃が暗号文となる。

【0106】

これを受信したBは、受信データを鍵K_{a b}で復号化する。受信データの復号化方法は、まず、暗号文E₁を鍵K_{a b}で復号化し、乱数R_aを得る。次に、暗号文E₂を鍵K_{a b}で復号化し、その結果とE₁を排他的論理和し、R_bを得る。最後に、暗号文E₃を鍵K_{a b}で復号化し、その結果とE₂を排他的論理和し、ID(b)を得る。こうして得られたR_a、R_b、ID(b)の内、R_bおよびID(b)が、Bが送信したものと一致するか検証する。この検証に通った場合、BはAを正当なものとして認証する。

【0107】

次にBは、認証後に使用するセッション鍵(Session Key(以下、K_{s e s}とする))を生成する(生成方法は、乱数を用いる)。そして、R_b、R_a、K_{s e s}の順に、DESのCBCモードで鍵K_{a b}を用いて暗号化し、Aに返送する。

【0108】

これを受信したAは、受信データを鍵K_{a b}で復号化する。受信データの復号化方法は、Bの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたR_b、R_a、K_{s e s}の内、R_bおよびR_aが、Aが送信したものと一致するか検証する。この検証に通った場合、AはBを正当なものとして認証する。互いに相手を認証した後には、セッション鍵K_{s e s}は、認証後の秘密通信のための共通鍵として利用される。

【0109】

なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0110】

次に、公開鍵暗号方式である160ビット長の楕円曲線暗号を用いた相互認証方法を、図11を用いて説明する。図11において、公開鍵暗号方式としてECCを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも160ビットでなくてもよい。図11において、まずBが、64ビットの乱数R_bを生成し、Aに送信する。これを受信したAは、新たに64ビットの乱数R_aおよび標数pより小さい乱数A_kを生成する。そして、ベースポイントGをA_k倍した点A_v=A_k×Gを求め、R_a、R_b、A_v(X座標とY座標)に対する電子署名A_{Sig}を生成し、Aの公開鍵証明書とともにBに返送する。ここで、R_aおよびR_bはそれぞれ64ビット、A_vのX座標とY座標がそれぞれ160ビットであるので、合計448ビットに対する電子署名を生成する。電子署名の生成方法は図8で説明したので、その詳細は省略する。

【0111】

公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局(IA)410の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局(IA)の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図9で説明したのでその詳細は省略する。

【0112】

図11に戻って説明を続ける。Aの公開鍵証明書、R_a、R_b、A_v、電子署名A_{Sig}を受信したBは、Aが送信してきたR_bが、Bが生成したものと一致するか検証する。その結果、一致していた場合には、Aの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Aの公開鍵を取り出す。そして、取り出したAの公開鍵を用い電子署名A_{Sig}を検証する。電子署名の検証方法は図9で説明したので、その詳細は省略する。電子署名の検証に成功した後、BはAを正当なものとして認証する。

【0113】

次に、Bは、標数pより小さい乱数B_kを生成する。そして、ベースポイント

G を $B k$ 倍した点 $B v = B k \times G$ を求め、 $R b$ 、 $R a$ 、 $B v$ （X座標とY座標）に対する電子署名 $B. Sig$ を生成し、 B の公開鍵証明書とともにAに返送する。

【0114】

B の公開鍵証明書、 $R b$ 、 $R a$ 、 $B v$ 、電子署名 $B. Sig$ を受信したAは、 B が送信してきた $R a$ が、Aが生成したものと一致するか検証する。その結果、一致していた場合には、 B の公開鍵証明書内の電子署名を認証局の公開鍵で検証し、 B の公開鍵を取り出す。そして、取り出した B の公開鍵を用い電子署名 $B. Sig$ を検証する。電子署名の検証に成功した後、Aは B を正当なものとして認証する。

【0115】

両者が認証に成功した場合には、 B は $B k \times A v$ （ $B k$ は乱数だが、 $A v$ は橍円曲線上の点であるため、橍円曲線上の点のスカラー倍計算が必要）を計算し、 A は $A k \times B v$ を計算し、これら点のX座標の下位64ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を64ビット鍵長の共通鍵暗号とした場合）。もちろん、Y座標からセッション鍵を生成してもよいし、下位64ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【0116】

電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【0117】

ユーザデバイス220、サービスプロバイダ240、クリアリングセンタ260と、口座管理機関280は、このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【0118】

ユーザデバイス220がコンテンツをサービスプロバイダ240に要求してコンテンツを受領する際のコンテンツ料金の支払処理は、電子マネー221の残高からコンテンツ料金を減額して、さらに、利用ログ情報として必要な情報、すな

わち、コンテンツの対価として支払った金額に対応する利用金額、料金の受け取り先情報、利用サービス情報、さらに、ユーザデバイス側で管理するシリアル番号等を記録した利用ログを生成してサービスプロバイダ240へ送信する処理となる。

【0119】

図4に戻り、本発明のコンテンツ取り引きシステムにおけるコンテンツの取り引き処理について説明を続ける。

【0120】

ユーザデバイス220は、コンテンツの提供者であるサービスプロバイダ240に対してコンテンツを要求（図4に示す（1）の処理）する。

【0121】

サービスプロバイダ240は、ユーザデバイス220から要求のあったコンテンツをユーザデバイスに送信（図4に示す（2）の処理）する。なお、ここで送信するコンテンツは、コンテンツデータをコンテンツ鍵によって暗号化した暗号化コンテンツである。サービスプロバイダ240は、暗号化コンテンツに加えて、コンテンツ料金およびコンテンツ料金の支払先情報としてのコンテンツの価格情報、さらに後段で説明するが、コンテンツの利用期限、複製可能回数等を販売条件情報（UCP：Usage Control Policy）として設定して、さらに電子署名を付してユーザデバイスに送信する。サービスプロバイダ240は、コンテンツの利用条件を各種設定可能である。これらの転送コンテンツ構成（セキュアコンテンツ）については後段で説明する。

【0122】

次に、ユーザデバイス220は、予め定められたコンテンツの使用料金に対応する金額を電子マネー221から引出してサービスプロバイダ240に支払う。

【0123】

これらの料金処理は、具体的には、図4に示すユーザデバイス220の有する電子マネー221の残高から利用料金を減額し、発行ログ情報と、コンテンツの利用金額、コンテンツの利用料金の受け取り先情報等を記録したデータからなる利用情報をデータとして持つ利用ログ252を生成してサービスプロバイダ24

0に送信（図4に示す（3）の処理）する処理として実行される。この利用ログデータの転送は、上述した通り、ユーザデバイス220とサービスプロバイダ240間の相互認証処理を実行し、ユーザデバイス220による電子署名がなされて転送する。

【0124】

サービスプロバイダ240は、ユーザデバイス220から受領した利用ログ252を検証して、データ正当性が確認されると、暗号化コンテンツの復号に用いるコンテンツ鍵を先に説明した認証処理の際に生成したセッション鍵で暗号化してユーザデバイス220に送信する。ユーザデバイスは、暗号化コンテンツ鍵をセッション鍵で復号して得たコンテンツ鍵を用いて暗号化コンテンツを復号して利用する。

【0125】

サービスプロバイダ240は、さらに、ユーザデバイス220から受領した利用ログ252に基づいて、図6で説明したコンテンツ利用料金の支払元、受領日時等からなる受領情報を持つ受領ログ253を生成してクリアリングセンタ260に送信（図4に示す（4）の処理）する。このデータ転送についても、サービスプロバイダ240とクリアリングセンタ260間の相互認証処理を実行し、サービスプロバイダ240による電子署名を行なってデータ転送が実行される。

【0126】

クリアリングセンタ260は、サービスプロバイダ240から受信した受領ログ253を検証して、データ正当性が確認されると、受領ログ253に基づいて電子マネーによる支払い処理、すなわち電子データ上での決済処理を行なうことになる。

【0127】

まず、クリアリングセンタ260は、受領ログ中のデータに基づいてユーザ管理サーバ中の対応するユーザデータを抽出し、クリアリングセンタ260が管理するユーザの電子マネーによる支払処理であることを確認する。さらに、クリアリングセンタ260は、決済処理に関する実際の現金の受け渡し情報を口座管理機関280に振替要求として送信（図4に示す（5）の処理）する。

【0128】

口座管理機関280は、クリアリングセンタ260からの振替要求に基づいて、サービスプロバイダ口座282、クリアリングセンタ管理下のユーザ電子マネー口座283相互間において、金額振替、振込処理を実行（図4に示す（6）の処理）する。なお、先に説明したように振込先は1つのプロバイダとは限らず、複数の関係先、例えばコンテンツ著作者、コンテンツ販売店等である場合にはその他の口座285に対する振込処理も実行される。また、これらの処理は複数の受領ログに対して一括して行なう場合もある。なお、図4に示す（6）の処理は、各口座が同一金融機関内にあれば、同一の金融機関（例えば銀行）内で行われるが、異なる金融機関に口座が存在する場合は、異なる金融機関の間での金額振替、振込処理として行われる。これらの金額配分に関しては、受領ログ中に記録されており、クリアリングセンタ260は、受領ログに記録された配分情報に従った振替要求を口座管理機関280に対して行なう。コンテンツ料金の配分については、後段で説明する。

【0129】

このコンテンツ利用料金配分情報は、図6の受領ログに含まれる利用ログ中の利用情報中の「受取先」、受領ログ中の受領情報の「支払元」情報であり、クリアリングセンタ260がこの情報に基づいて振替構成を決定して、口座管理機関280に対して振替要求を行なうことになる。

【0130】

口座管理機関280による金額移動としての金額振替、振込処理が実行されると、口座管理機関280は、振替処理確認応答をクリアリングセンタ260に送信（図4に示す（7）の処理）する。

【0131】

振替処理確認応答を受信したクリアリングセンタ260は、決済サーバ262に格納した決済データを更新して電子マネーの決済処理を実行（図4に示す（8）の処理）するとともに、各ユーザの電子マネー残高を登録しているユーザ残高管理サーバ263の残高データの更新処理を実行（図4に示す（9）の処理）する。これらの処理が正常に実行されると、クリアリングセンタ260のユーザ残

高管理サーバ263の残高と、口座管理機関280のクリアリングセンタ管理下のユーザ電子マネー口座283との残高が一致することになる。

【0132】

[4. 二次配布を可能としたコンテンツ構成]

本発明のコンテンツ取り引きシステムでは配布するコンテンツを以下に説明する構成とすることで、複数の異なるユーザ間においてコンテンツの配信を可能とし、かつユーザ間の配信においてもコンテンツ利用料金を回収することが可能とした構成を持つ。

【0133】

以下で説明するユーザ間のコンテンツ配信の形態には2つの形態がある。1つは、ユーザAからユーザB、さらにユーザBからユーザC等、直列的に異なるユーザ間をコンテンツが順次、取り引きされる形態である。この直列的なユーザ間のコンテンツ配信を以下、「世代間配信」と呼ぶ。もう1つの配信形態は、ユーザAの購入したコンテンツをユーザAからユーザB, C, D等、並列的に配信する形態である。すなわち1人のユーザから複数のユーザに並列に同一コンテンツを配信する形態である。この並列的なコンテンツ配信を、以下「二次配信」と呼ぶ。

【0134】

図12に本発明のコンテンツ取り引きシステムにおいて流通するコンテンツを含むセキュア・コンテナ(Secure Container)の構成を示す。図12に示すようにセキュアコンテナは、コンテンツ鍵によって暗号化されたコンテンツ1201と、コンテンツの料金とコンテンツ料金の受け取り先、配分情報を含む価格情報1202と、コンテンツの利用条件、例えば「世代間配信」「二次配信」等の転売が禁止されている1回限りの配信が許容されたコンテンツであるとか、複数回の転売が可能であるとか、複数回の転売が可能である場合の転売条件、例えば2回までの「世代間配信」と、3回までの「二次配信」が許容されているコンテンツであるとか、あるいは利用可能期間等の設定情報としての販売条件(UCP)1203と、セキュアコンテナの作成者の電子署名1204を含んで構成される。

【0135】

価格情報1202、販売条件1203は、コンテンツ製作者、コンテンツプロバイダ、サービスプロバイダ等のいずれかが設定する、電子署名は、コンテンツの流通を管理する機関による署名である。コンテンツの流通を管理する機関がサービスプロバイダであれば、サービスプロバイダの署名となる。

【0136】

図13に販売条件(UCP)1203の具体的構成例、図14に価格情報1202の具体的構成例を示す。図13に示すように販売条件(UCP)には、コンテンツ識別子(ID)、コンテンツの利用可能なユーザデバイスを設定した使用可能機器条件、コンテンツの利用可能な地域を設定した地域コード、どのようにコンテンツを利用してよいかを示す利用権タイプ(例えばコンテンツの再生可能回数、コンテンツの複製(ダウンロード)可能回数)、異なるユーザデバイス間での流通可能回数として、前述した「世代間配信」の可能回数を設定した「UCP世代管理情報」1301と、前述の「二次配信」の可能回数を設定した「二次配信可能回数」1302が含まれる。「UCP世代管理情報」に設定されたそれぞれのユーザ間での配信可能回数は、ユーザデバイス内のメモリにコンテンツに応じて格納される使用制御情報(UCS:Usage Control Status)(図16参照)中の「UCS世代管理情報」、「UCS二次配信可能回数」の元データとなり、「UCS世代管理情報」、「UCS二次配信可能回数」に基づいてそれぞれの処理の可否が決定される。「UCS世代管理情報」はコンテンツの世代間配信毎に更新され、「UCS二次配信可能回数」はコンテンツの二次配信毎に更新される。

【0137】

ユーザデバイス内のUCSに記録される「UCS世代管理情報」に基づいて世代間配信の可否が決定される。すなわち、セキュアコンテンツ内の販売条件(UCP)の「UCP世代管理情報」に設定された世代間配信可能回数を制限回数としてコンテンツの世代間配信が可能となる。それ以上のコンテンツの世代間配信はエラーとなり、実行されない。同様に、ユーザデバイス内のUCSに記録された「UCS二次配信可能回数」に基づいて二次配信の可否が決定される。すなわ

ち、セキュアコンテンツ内の販売条件（UCP）の「UCP二次配信可能回数」に設定された二次配信可能回数を制限回数としてコンテンツの二次配信が可能となる。それ以上のコンテンツの二次配信はエラーとなり、実行されない。

【0138】

さらに後段で説明するが、「UCS世代管理情報」は、世代間配信、つまりユーザ間のコンテンツ取り引き（セキュアコンテナの転送）の際にユーザ間において継承されてコンテンツの提供を受けたユーザデバイスBにおいて、コンテンツ供給元のユーザデバイスAのUCS（A）に基づいて、UCS（A）の「UCS世代管理情報」を引き継いだ新たなUCS（B）が生成される。例えばUCS（A）の「UCS世代管理情報」が5であったとき、ユーザデバイスAからユーザデバイスBに対する世代間配信により、1回の世代間配信が実行されるので、ユーザデバイスBに生成されるUCS（B）の「UCS世代管理情報」は4に設定される。これらの処理については、後段で詳細に説明する。

【0139】

また、「UCS二次配信可能回数」についても、二次配信を行なったユーザ間で、その情報を引き継いで、二次配信を受けたユーザデバイスにおいて、「UCS二次配信可能回数」を1つ減少、すなわちデクリメントして新たなUCSを生成して格納する。

【0140】

あるいは、二次配信に関しては、ユーザ間での「UCS二次配信可能回数」の情報の継承を行なわず、二次配信を受けたユーザデバイスにおいて、セキュアコンテナの「UCP二次配信可能回数」を再度有効にする構成としてもよい。すなわち、「UCP二次配信可能回数」が5回として設定されている場合、そのコンテンツを新たに受領したユーザは常に5回のコンテンツの二次配信が可能になるように構成してもよい。

【0141】

世代間配信と二次配信の継承の例について説明する。サービスプロバイダから最初にコンテンツを購入したユーザ（A）は、セキュアコンテナ中のUCPにある「UCP世代管理情報」と「UCP二次配信可能回数」に基づいて「UCS世

代管理情報」と「UCS二次配信可能回数」を有するUCSを生成して格納する。例えば「UCP世代管理情報」=3、「UCP二次配信可能回数」=5であったとすると、ユーザAのUCSは、「UCS世代管理情報」=3、「UCS二次配信可能回数」=5として生成される。

【0142】

ユーザ(A)がユーザ(B)にコンテンツを配信すると、ユーザAの「UCS世代管理情報」=3、「UCS二次配信可能回数」=4となり、ユーザBに生成されるUCSは「UCS世代管理情報」=2、「UCS二次配信可能回数」=5(継承する場合4)となる。

【0143】

さらに、ユーザ(A)がユーザ(C)にコンテンツを配信すると、ユーザAの「UCS世代管理情報」=3、「UCS二次配信可能回数」=3となり、ユーザCに生成されるUCSは「UCS世代管理情報」=2、「UCS二次配信可能回数」=5(継承する場合3)となる。

【0144】

さらに、ユーザ(B)がユーザ(D)にコンテンツを配信すると、ユーザBの「UCS世代管理情報」=2、「UCS二次配信可能回数」=4(継承している場合3)となり、ユーザDに生成されるUCSは「UCS世代管理情報」=1、「UCS二次配信可能回数」=5(継承する場合3)となる。

【0145】

さらに、ユーザ(D)がユーザ(E)にコンテンツを配信すると、ユーザDの「UCS世代管理情報」=1、「UCS二次配信可能回数」=4(継承している場合2)となり、ユーザEに生成されるUCSは「UCS世代管理情報」=0、「UCS二次配信可能回数」=5(継承する場合2)となる。

【0146】

ここで、ユーザ(E)は、「UCS世代管理情報」=0であるので、「UCS二次配信可能回数」の設定数に無関係に新たな配信はできない。ユーザ(A)は、ユーザ(B)と(C)に配信を行なっており、「UCS二次配信可能回数」=3であり、あと3回の配信が可能である。また、ユーザ(B)は、ユーザ(D)

に配信を行なっており、「UCS二次配信可能回数」 = 4（継承している場合3）であり、あと4回（継承している場合3回）の配信が可能である。また、ユーザー（C）は、配信を行なっておらず、「UCS二次配信可能回数」 = 5（継承している場合3）であり、あと5回（継承している場合3回）の配信が可能である。ユーザー（D）は、ユーザー（E）に配信を行なっており、「UCS二次配信可能回数」 = 4（継承している場合2）であり、あと4回（継承している場合2回）の配信が可能となる。

【0147】

このように、「UCS世代管理情報」 = 0になったUCSを持つユーザデバイスは、それ以上、他のユーザデバイスに対してコンテンツの配布が実行できなくなるが、「UCS世代管理情報」 = 1以上であれば、そのユーザは、「UCS二次配信可能回数」に設定された回数のコンテンツ配布が可能となる。

【0148】

図13の販売条件（UCP）には、さらに、ルール1～Nとして、異なるコンテンツ利用条件が設定されている。これらは、ユーザ、ユーザデバイスに応じて、あるいはユーザが選択可能なコンテンツ利用条件を複数設定したものであり、各ルールに従って例えばコンテンツ価格等が異なるように設定されている。

【0149】

図14は、図12のセキュアコンテナの価格情報のを例を示すものであり、図13の販売条件（UCP）と同様のコンテンツID等の情報の他に、価格情報ID、価格情報バージョンが含まれ、さらに、図13の販売条件（UCP）と同様、ルール1～Nとして、異なるコンテンツ利用価格が設定されている。各ルールには、それぞれのコンテンツ利用価格、コンテンツ利益配分情報が設定されている。

【0150】

先に、図6で説明した利用ログ、および受領ログのコンテンツ利用料金の支払先に関する情報は、上述したセキュアコンテナの販売条件（UCP）、価格情報に基づいて生成されるものである。

【0151】

図12に示すセキュアコンテナを流通コンテンツデータとすることにより、複数のユーザ間での二次配信を可能とした決済処理構成を図15に示す。

【0152】

図15において、ユーザデバイスAは、サービスプロバイダ240に対してコンテンツの要求を行ない、前述したと同様の認証処理、署名検証処理等を実行して、コンテンツ利用料金の支払い処理として発行ログA1531に基づいて利用ログA1532を生成してサービスプロバイダ240に送信する。

【0153】

なお、この転送コンテンツは、図12で説明したように、コンテンツ鍵で暗号化されたものであり、サービスプロバイダ240は、利用ログAの署名検証を確認した後、ユーザデバイスA1510に対して、コンテンツ鍵を暗号化して送信する。暗号化処理用の鍵としては、認証処理時に生成するセッション鍵を使用する。具体的な処理の流れを簡単に説明すると、（1）サービスプロバイダ240とユーザデバイスA1510間での相互認証処理、（2）サービスプロバイダ240からユーザデバイスA1510へのセキュアコンテナ送信、（3）ユーザデバイスA1510におけるセキュアコンテナの署名検証、（4）ユーザデバイスA1510において、販売条件（UCP）、ライステグ（PT）から購入判断、（5）ユーザデバイスA1510の電子マネーで支払処理、（6）サービスプロバイダ240からユーザデバイスA1510へコンテンツ鍵送信、（7）ユーザデバイスA1510において使用制御情報（UCS：Usage Control Status）を生成して保存（コンテンツ鍵保存）の一連の処理となる。なお、サービスプロバイダ240とユーザデバイスA1510間で相互認証処理は、（4）のユーザデバイスA1510における購入判断処理後、（5）のユーザデバイスA1510の電子マネーによる支払処理の前に実行するようにしてもよい。

【0154】

ユーザデバイスA1510は、受領したセキュアコンテナの暗号化コンテンツをコンテンツ鍵によって復号して利用することが可能となる。ユーザデバイスA1510は、コンテンツを利用する際、すなわちコンテンツのコンテンツ鍵を用いた復号処理の実行に先立ち、ユーザデバイスに格納されたコンテンツ利用の可

否の判定に利用されるUCS (Usage Control Status : 使用制御情報) を検査しコンテンツを利用できるか判定する。なお、UCSは、コンテンツの購入処理、すなわち電子マネーによる支払いをサービスプロバイダ240に対して実行する際に、ユーザデバイス内の暗号処理部において、UCPに基づいて生成され、ユーザデバイス内のメモリに格納される。この処理については、図16において説明する。ユーザデバイスにおけるセキュアコンテナ格納コンテンツの復号処理は、UCSを検査した結果、コンテンツを利用できると判定されたときのみ実行可能となる。

【0155】

ユーザデバイスの暗号処理部は、UCSが条件をクリアするものである場合にのみ、コンテンツの復号処理を実行し、UCSが条件をクリアしない場合には、エラーとして復号処理を実行しない。ユーザデバイスには、このようにユーザデバイスに設定されたUCSが利用条件をクリアした場合にのみ復号処理を実行可能とするコンテンツ利用判定プログラムが格納される。このコンテンツ利用判定プログラムは、例えばセキュアコンテナを提供するサービスプロバイダによって提供され、ユーザデバイスにおいてコンテンツ鍵による復号処理を実行する前ステップで実行するように設定される。

【0156】

図16にコンテンツに応じてユーザデバイスにおいて生成されユーザデバイス内のメモリに格納される使用制御情報 (UCS : Usage Control Status) の例を示す。図16に示すように、使用制御情報 (UCS) には、コンテンツID、サービスプロバイダID等の情報の他に、再生残り回数、複製残り回数等のコンテンツ利用の制限情報が含まれる。これら、再生残り回数、複製残り回数は、同一のユーザデバイス内で利用可能な再生残り回数、複製残り回数を示すデータである。さらに使用制御情報 (UCS) には、「UCS世代管理情報」1601、および「UCS二次配信可能回数」1602が含まれる。

【0157】

「UCS世代管理情報」は前述したように、「世代間配信」の可能回数を設定したものであり、コンテンツを最初に購入したユーザデバイスは、図13の「U

「CP世代管理情報」1301に一致する回数が設定され、ユーザからの世代間配信によってコンテンツを受領したユーザデバイスは、同一セキュアコンテナについてすでに実行された世代間配信の回数が減じられた回数が設定される。

【0158】

「UCS二次配信可能回数」1602は前述の「二次配信」の可能回数を設定したフィールドであり、コンテンツを最初に購入したユーザデバイスは、図13の「UCP二次配信可能回数」1302に一致する回数が設定され、その後の二次配信に応じて更新、すなわち設定回数がデクリメントされる。

【0159】

この「UCS二次配信可能回数」1602は、前述したようにユーザ間のコンテンツ取り引きにおいて、そのデータを継承する構成と、継承しない構成がある。

【0160】

このように、コンテンツのユーザ間での配信は、ユーザデバイス内のメモリにコンテンツに応じて格納される使用制御情報（UCS：Usage Control Status）中の「UCS世代管理情報」、「UCS二次配信可能回数」に基づいて、それぞれの処理の可否が決定される。「UCS世代管理情報」はコンテンツの世代間配信毎に更新され、「UCS二次配信可能回数」はコンテンツの二次配信毎に更新される。

【0161】

同一のセキュアコンテナを異なるユーザ間で転送して取り引きを行なう際、UCSの「UCS世代管理情報」は、コンテンツ提供元からコンテンツ提供先に継承され、コンテンツ提供先において生成されるUCS内に格納される。「UCS二次配信可能回数」は継承する構成と継承しない構成がある。

【0162】

「UCS世代管理情報」に記録された利用制限情報は、同一のセキュアコンテナ内のコンテンツについての利用を異なるユーザデバイスで行なった場合も、逐次更新されるデータとなる。例えば、3回の世代間配信制限がセキュアコンテナの販売条件（UCP）に設定されている場合、最初のセキュアコンテナ購入者（

ユーザデバイスA)の「UCS世代管理情報」には、まず3回の世代間配信が可能として設定されるが、ユーザAがユーザBにコンテンツ配信を実行すると、ユーザBの「UCS世代管理情報」は2として設定される。

【0163】

このように、セキュアコンテナの販売条件(UCP)の「UCP世代管理情報」、「UCP二次配信可能回数」には、流通回数上限が設定されている。ユーザデバイスに生成されるUCSにも「UCS世代管理情報」、「UCS二次配信可能回数」が格納され、前述のコンテンツ利用判定プログラムは、「UCS世代管理情報」、「UCS二次配信可能回数」を参照して、設定された流通回数の上限値を超えて、異なるユーザデバイスにセキュアコンテナを送信する場合に、その送信処理の前ステップとして実行されるコンテンツ利用判定プログラムにより、設定回数以上の流通であると判定されると、処理エラーとなりコンテンツの送信処理が実行されない。「UCP世代管理情報」、「UCS二次配信可能回数」に設定された流通回数の上限値を超えない場合にのみ、コンテンツのユーザデバイス間での送信処理に移行し、コンテンツの世代間配信または二次配信が可能となる。すなわち、ユーザデバイス間での転送(世代間配信または二次配信)は、セキュアコンテナの生成時に販売条件(UCP)として設定された「UCP世代管理情報」、および「UCP二次配信可能回数」での条件の範囲内でのみ可能となる。

【0164】

図15に戻って、ユーザ間でのコンテンツ配信におけるコンテンツ提供ユーザデバイスからの受領ログの発行によるコンテンツ利用料金回収構成について説明する。

【0165】

図15では、まず、サービスプロバイダ240から、ユーザデバイスAに対してセキュアコンテナとしてのコンテンツが提供され、ユーザデバイスAは、電子マネー1511によりコンテンツ利用料金を支払う。具体的には、ユーザデバイスAは、セキュアコンテナ中の価格情報、販売条件、発行ログA1531に基づいて、利用ログA1532を生成して、これをサービスプロバイダに転送し、サ

サービスプロバイダ240は、利用ログA1532に基づいて受領ログA1533を生成してクリアリングセンタ260に受領ログA1533を転送して、クリアリングセンタ260が受領ログに基づいて決済処理を行なう。実際の利用料金の振替はクリアリングセンタ260の振替要求に基づいて口座管理機関280が実行する。

【0166】

先に図6を用いて簡単に受領ログの構成について説明したが、受領ログを構成する受領情報の他の具体例を図17に示す。受領情報には、コンテンツ利用料金の配分情報が含まれる。図17の受領情報のデータ部1701には、コンテンツプロバイダの利益額／利益率、サービスプロバイダの利益額／利益率、その他の関係者の利益額／利益率が記録されている。ここで示す受領情報は一例であり、例えば二次配信を実行したユーザデバイス、あるいはユーザデバイスを管理する管理ユーザに対して利益配分を設定してもよく、あるいはコンテンツの販売がCD、DVD等のメディアを介して行われる場合には、その販売店に対する利益配分を設定したり、クリアリングセンタに利益配分を設定したり、あるいはコンテンツ著作者に対する利益配分を設定する構成が可能である。

【0167】

これらの受領情報に設定される利益配分情報は、セキュアコンテナの価格情報（図14参照）、販売条件（図13参照）に基づいて設定される情報であり、セキュアコンテナの生成時に配分情報を設定してコンテンツを流通させる。クリアリングセンタは、受領情報に記録された配分情報に従って、決済処理構成を構築して、これに基づいて振替要求を口座管理機関280に出力し、口座管理機関280は要求に従った振替処理を実行する。一方、受領情報としては図6に示すようなものとし、クリアリングセンタ260は、売上げのすべてをサービスプロバイダに支払い、サービスプロバイダ240がコンテンツプロバイダ、他に利益分配を行なうように構成してもよい。

【0168】

また、図17に示すように受領情報には、セキュアコンテナの販売条件に含まれる「UCP世代管理情報」1702が格納され、クリアリングセンタは、受領

情報に記録された「UCP世代管理情報」と同一コンテナに基づく受領ログの発行数を比較し、「UCP世代管理情報」の設定を超える受領ログについては、その受領ログを無効として処理を行なわない。

【0169】

このように、サービスプロバイダ240がセキュアコンテナを流通させることにより、セキュアコンテナに記録されたデータに従って、コンテンツの利用がなされ、かつその利用にともなって受領ログが発行されて、発行された受領ログに基づいて正確なコンテンツ利用料金の回収が自動的に行われる。

【0170】

さらに、図15を用いて異なるユーザデバイス間でのコンテンツ流通について説明する。ユーザデバイスA1510が取得し、例えば所定回数の再生、あるいはダウンロード処理を行なったセキュアコンテナは、異なるユーザデバイスB1520に転送することが可能である。ただし、世代間配信または二次配信が可能なコンテンツは、前述のようにセキュアコンテナの販売条件の「UCP世代管理情報」、「UCP二次配信可能回数」が二次配信を可能として設定している場合のみである。この場合、セキュアコンテナは、ユーザデバイスB1520に転送することが可能である。ただし、転送は前述のように「UCS世代管理情報」、「UCS二次配信可能回数」の設定回数の制限範囲内に場合にのみ可能であり、これはコンテンツ利用判定プログラムによって制御されることになる。なお、ユーザデバイス間でのデータ転送においても、前述の認証処理、セッション鍵生成、さらに、転送データの署名検証処理が実行される。

【0171】

ユーザデバイスB1520は、セキュアコンテナを受信し、購入処理を実行すると発行ログB1551に基づいて、利用ログB1552を生成して、これをユーザデバイスA1510に転送し電子マネー1521による支払処理を行なう。ユーザデバイスA1510は、利用ログB1552に基づいて受領ログB1553を生成してクリアリングセンタ260に受領ログBを転送して、クリアリングセンタ260が受領ログBに基づいて決済処理を行なう。実際の利用料金の振替はクリアリングセンタ260の振替要求に基づいて口座管理機関280が行なう

。この場合の受領ログBにも、前述の図17で説明したと同様のコンテンツ利用料金配分情報が含まれており、クリアリングセンタ260は、受領ログ中のコンテンツ利用料金配分情報に基づいてユーザデバイスB1520のコンテンツ利用に基づく利用料金配分を実行する。

【0172】

セキュアコンテナは、先にも説明したようにコンテナの販売条件(UCP)に設定された制限に至るまでユーザ間での流通が可能であり、その範囲内であれば、図15に示すようにユーザデバイスB1520から、さらに他のユーザデバイスC1570にコンテンツを有するセキュアコンテナを流通させることが可能となる。この場合は、ユーザデバイスB1520が、ユーザデバイスC1570からの利用ログに基づいて受領ログを生成してクリアリングセンタ260に受領ログを送信し、決済を行なう。

【0173】

なお、図15に示すように受領ログは、サービスプロバイダ240に送信し、二次配信においては、コンテンツの利用料金の決済処理を行なうのではなく、サービスプロバイダ240がコンテンツの提供ユーザに何らかの特典を付与するためのポイントを与えるように構成してもよい。このポイント付与構成については、後段で説明する。

【0174】

図18にユーザデバイス間でのセキュアコンテナの転送処理を実行するユーザデバイス構成を中心としたブロック図を示す。図18を用いてセキュアコンテナの転送、コンテンツ使用制御情報(UCS)生成、格納処理について説明する。

【0175】

図18のサービスプロバイダ1810が、セキュアコンテナの最初の流通(一次配布)を行なう。サービスプロバイダ1810は、コンテンツデータベース1812にコンテンツを格納し、さらに、ユーザ情報データベース1813にユーザ情報を格納している。サービスプロバイダ1810は、制御部1811の制御のもとに暗号処理部1814において、セキュアコンテナの転送処理に必要な転送先との相互認証処理、転送データに対する署名処理等を実行する。暗号処理部

1814は、これら各暗号処理に必要となる鍵情報、さらに、先に説明した公開鍵証明書発行局（IA）の公開鍵、公開鍵証明書発行局（IA）の発行した公開鍵証明書等を保持したメモリを有している。

【0176】

また、図18に示すクリアリングセンタ1840がコンテンツ流通に伴うコンテンツ利用料の決済（電子マネー上のデータ）処理を行なう。クリアリングセンタ1840は、通信部1845を介して行われる決済用の受領ログ受信または発行ログ送信において各デバイスと認証処理を実行し、また送受信データに対する署名処理、署名検証処理を実行するための暗号処理部1844を有し、また、前述の図2、図4等を用いて説明したユーザ管理、ユーザ残高管理用の各種のデータを格納したデータベース1842を有する。暗号処理部1844には、各暗号処理に必要となる鍵情報、公開鍵証明書発行局（IA）の公開鍵、公開鍵証明書発行局（IA）の発行した公開鍵証明書等を保持したメモリを有している。制御部1841は、データ送受信、暗号処理部における暗号処理時のデータ転送等の制御を行なう。

【0177】

サービスプロバイダ1810は、ユーザデバイスA1820に対してセキュアコンテナを通信部1815を介して転送して、ユーザデバイスA1820が通信部1827を介してこれを受信し、購入処理を実行すると、ユーザデバイスA1820は、制御部1821の制御のもとに暗号処理部1822においてセキュアコンテナの販売条件（UCP）等に基づいてコンテンツ使用制限情報（UCS）を生成して、これをフラッシュメモリ等のメモリ1824に格納する。

【0178】

ユーザデバイスA1820は、電子マネー1828によるコンテンツ利用料金支払処理、すなわち前述した利用ログを暗号処理部1822において生成して、通信部1827を介してサービスプロバイダ1810に送信する。ユーザデバイスA1820が受信したセキュアコンテナは、ハードディスク等の記憶部1825に格納される。サービスプロバイダ1810は、ユーザデバイスA1820から送信された利用ログの検証をして、検証が済むと、コンテンツ鍵をセッション

鍵で暗号化してユーザデバイスA1820に送信する。ユーザデバイスA1820は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイスA1820固有の保存鍵で暗号化してメモリ1824に格納する。

【0179】

ユーザデバイスA1820は、データ再生部1826でのコンテンツ再生等、コンテンツ利用に際しては、メモリ1824に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部1825に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部1826において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、その前ステップとして、メモリ1824に格納されたコンテンツ使用制限情報（UCS）の再生残り回数等の設定条件を判定し、条件がクリアされた場合には復号が可能となる。

【0180】

さらに、セキュアコンテナをユーザデバイスA1820からユーザデバイスB1830に配信する場合は、ユーザデバイスA1820は、メモリ1824からコンテンツ使用制限情報（UCS）を読み出し、暗号処理部1822内で保存鍵で復号化（暗号化されていない場合は復号処理は不要）し、UCSの「UCS世代管理情報」、「UCS二次配信可能回数」を判定し、新たな配信が可能と判定された場合には、ユーザデバイスB1830に対してセキュアコンテナを通信部1827を介して転送して、ユーザデバイスB1830が通信部1837を介してこれを受信し、購入処理を実行する。ユーザデバイスB1830は、制御部1831の制御のもとに暗号処理部1832においてセキュアコンテナの販売条件（UCP）とユーザデバイスA1820のUCS情報等に基づいて、新たな「UCS世代管理情報」、「UCS二次配信可能回数」を設定したコンテンツ使用制限情報（UCS-B）を生成して、これをフラッシュメモリ等のメモリ1834に格納する。

【0181】

この際に生成するUCS-Bは、前述した通り、ユーザデバイスA1820のコンテンツ利用履歴を継承したものとなる。前述の通り、UCS-Bの「UCS

「世代管理情報」はUCS-Aの「UCS世代管理情報」より1つ減じた回数として設定される。UCS-Bの「UCS二次配信可能回数」はUCS-Aの「UCS二次配信可能回数」より1つ減じた回数として設定する構成と、セキュアコンテナ内の「UCP二次配信可能回数」と同一回数を新たに設定する構成がある。

【0182】

ユーザデバイスB1830は、電子マネー1838によるコンテンツ利用料金支払処理、すなわち前述した利用ログを暗号処理部1832において生成して、通信部1837を介してユーザデバイスA1820に送信する。ユーザデバイスB1830が受信したセキュアコンテナは、ハードディスク等の記憶部1835に格納される。ユーザデバイスA1820は、ユーザデバイスB1830から送信された利用ログの検証をして、検証が済むと、メモリ1824からコンテンツ鍵を読み出し、これを保存鍵で復号した後、コンテンツ鍵をセッション鍵で暗号化してユーザデバイスB1830に送信する。ユーザデバイスB1830は、暗号化されたコンテンツ鍵をセッション鍵で復号し、これをさらにユーザデバイスB1830固有の保存鍵で暗号化してメモリ1834に格納する。

【0183】

また、不正な改竄により設定を超えた使用を行なうと、同一セキュアコンテナに基づいて生成された受領ログ数が、セキュアコンテナ中の販売条件(UCP)に含まれる「UCP世代管理情報」の設定を超えることとなるため、クリアリングセンタ1840に送付された場合に無効と判定される。図17に示すように受領ログには、コンテンツID等の情報とともに、セキュアコンテナに記録された「UCP世代管理情報」が記録されており、クリアリングセンタ1840における決済処理においては、「UCP世代管理情報」の設定を超える受領ログを受信した場合はこれを無効とする。なお、ユーザ間配信の認められない設定のなされたコンテンツに基づいて生成された受領ログについても、その受領ログを無効とする処理を実行する。

【0184】

ユーザデバイスB1830は、データ再生部1836でのコンテンツ再生等、

コンテンツ利用に際しては、メモリ1834に保存したコンテンツ鍵を保存鍵で復号して、復号したコンテンツ鍵を用いて記憶部1835に格納されたセキュアコンテナ中のコンテンツを復号処理してデータ再生部1836において再生する。なお、セキュアコンテナ中のコンテンツの復号処理に際しては、先に説明したように、その前ステップとして、メモリ1834に格納されたコンテンツ使用制限情報（UCS）に設定された再生残り回数等の利用可能状況が判定され、設定条件範囲内でコンテンツの利用、すなわち復号が可能となる。

【0185】

これらの処理により、セキュアコンテナは、サービスプロバイダとユーザデバイス間の一次配布、さらに複数のユーザデバイス間での二次配布（世代間配信または二次配信）が可能となり、そのコンテンツ利用は、セキュアコンテナ中の販売条件（UCP）に含まれる「UCP世代管理情報」、「UCP二次配信可能回数」によって制限された範囲で可能となる。また一次配布、二次配布（世代間配信または二次配信）に伴うコンテンツ利用料金回収もセキュアコンテナ中の価格情報、販売条件等に基づいて生成される受領ログに従って自動的に処理可能となるため、決済処理のための新たな処理が不要となる。

【0186】

次に、図19を用いてコンテンツの世代間配信、二次配信を行なう場合のコンテンツ供給側であるユーザデバイスAと、コンテンツ受領側であるユーザデバイスBの主要な処理フローについて説明する。

【0187】

まず、ステップS1901においてユーザデバイスAとユーザデバイスBとの間の相互認証処理（図10、図11参照）が実行される。この相互認証処理においてセッション鍵が生成される。ステップS1902において相互認証が成立しなかったと判定された場合は、エラーとなり、その後の処理は継続されない。必要であれば、相互認証処理のリトライを実行する。

【0188】

相互認証が成立すると、ステップS1903においてユーザデバイスAがハードディスク等の記憶媒体からセキュアコンテナを読み出し、さらにステップS1

904でフラッシュメモリ等のメモリに格納されたコンテンツ使用制限情報（UCS（A））を読み出す。

【0189】

ステップS1905において、ユーザデバイスAは、セキュアコンテナとコンテンツ使用制限情報（UCS）とをユーザデバイスBに送信する。この送信において、ユーザデバイスAは、送信データに対する署名処理を行なう。なお、コンテンツ使用制限情報（UCS（A））全体を送付することは必須ではなく、前述した「UCS世代管理情報」等、更新データとして引き継ぐ必要のあるデータのみをコンテンツ使用制限情報（UCS（A））から選択してユーザデバイスBに送付する構成としてもよい。

【0190】

ステップS1906において、ユーザデバイスBは、ユーザデバイスAから送付されたセキュアコンテナ、コンテンツ使用制限情報（UCS（A））の署名検証を実行する。検証が成立しなかった場合は、エラーとなり、処理は継続せず終了する。

【0191】

ステップS1907において、ユーザデバイスBは、電子マネーによるコンテンツ利用料金を支払う。この際の支払料金は、セキュアコンテナの価格情報、販売条件に規定されたものとなる。ユーザデバイスBの具体的な処理は、利用ログを生成してデバイスAに送付する処理となる。この際、利用ログにはユーザデバイスBの署名が付加される。

【0192】

次にステップS1908において、ユーザデバイスAがユーザデバイスBから送付された利用ログの署名検証を実行する。検証が成立しなかった場合は、エラーとなり、処理は継続せず終了する。

【0193】

ステップS1909では、ユーザデバイスAがメモリから保存鍵（ユーザデバイスAの暗号処理部のメモリに格納されている）で暗号化されたコンテンツ鍵を取り出して、保存鍵を用いた復号処理を実行し、さらにセッション鍵（ステップ

S1901の認証処理の際に生成)で再暗号化し、ステップS1910において、セッション鍵で暗号化したコンテンツ鍵をユーザデバイスBに送信する。

【0194】

ステップS1911において、ユーザデバイスBは、ユーザデバイスAから受信したコンテンツ使用制限情報(UCS(A))に基づいて、世代管理情報(または世代管理情報+二次配信可能回数)を引き継いだ新たなコンテンツ使用制限情報(UCS(B))を生成し、さらに、ユーザデバイスAから受信したセッション鍵で暗号化されたコンテンツ鍵をセッション鍵で復号し、さらに、ユーザデバイスBの暗号処理部のメモリに格納されている保存鍵で再暗号化する。ステップS1912では、コンテンツ使用制限情報(UCS(B))と、保存鍵で暗号化したコンテンツ鍵をフラッシュメモリ等のメモリに格納する。

【0195】

ステップS1913では、ユーザデバイスAが、ユーザデバイスBから受領した利用ログに基づいて受領ログを生成してこれをクリアリングセンタに送信する。なお、この受領ログにはユーザデバイスAの署名が付けられる。クリアリングセンタは署名検証の後、受領ログに基づく決済処理を行なう。なお、先にも述べたように受領ログに基づく決済処理の代わりにコンテンツの二次配布を行なったユーザデバイス、あるいはユーザデバイスの管理をする管理ユーザに対して何らかの優待ポイントを設定する処理を例えばサービスプロバイダにおいて実行する構成とした場合には、受領ログをサービスプロバイダに送信して、サービスプロバイダ側のユーザデータベースにおいてポイント付加処理を実行するようにしてもよい。なお、受領ログはすぐに送信せず、電子マネーを記録管理するメモリ内に保存しておく、適宜、例えば所定数の受領ログを蓄積した後、あるいは所定期間毎等、適当なタイミングで送信処理を実行するようにしてもよい。

【0196】

[5. コンテンツ二次配布におけるポイント付加処理]

これまでに説明したように、ユーザデバイス間でのセキュアコンテナを用いたコンテンツの二次配布は、受領ログによってすべて把握管理することが可能である。

【0197】

ここでは、受領ログを用いてコンテンツの二次配布を行なったユーザに対して何らかの特典を付与するための優待ポイントを二次配布時のコンテンツ提供者であるユーザデバイスあるいはユーザデバイスを管理する管理ユーザに付与することにより、ユーザ間のコンテンツの二次流通をより活性化させる構成について説明する。

【0198】

上述した構成においては、受領ログに含まれる受領情報（図17参照）に、コンテンツプロバイダの利益額／利益率、サービスプロバイダの利益額／利益率等を記録し、クリアリングセンタがこれらのデータに基づいて、コンテンツ利用料金の決済処理、具体的には、コンテンツプロバイダ、サービスプロバイダ、その他コンテンツ販売店舗、コンテンツ著作者に対してユーザから支払われたコンテンツ利用料金を配分する処理を実行していた。

【0199】

先に、図6、図17を用いて説明した受領情報に二次配布を実行したユーザデバイス、あるいはユーザデバイスを管理する管理ユーザに対するポイント付加情報を設定し、ポイント付加情報を含む受領情報を有する受領ログを、例えばサービスプロバイダに送信する（図15参照）構成とすることにより、サービスプロバイダが二次配布を実行したユーザデバイスあるいは二次配布を実行したユーザデバイスを管理する管理ユーザに対して何らかの優待ポイントを付加することが可能となる。優待ポイントは、例えば1つのセキュアコンテナの1回の二次配布につき1ポイントとして、ポイント数に応じて、新たなコンテンツの提供価格の割引を行なう。あるいはコンテンツの利用制限の緩和、例えば再生制限回数等を増加して設定する等の処理が可能となる。

【0200】

優待ポイントの処理を実行するのは、サービスプロバイダ、クリアリングセンタ、コンテンツプロバイダ、あるいは別のサービス機関によって行なわってもよいが、ここではサービスプロバイダがポイント処理を行なう例について説明する。図20にポイント処理を説明するブロック図を示す。

【0201】

図20において、No. 1～No. 5は、時系列的な処理順を示している。No. 1、No. 2の処理は先の図15において説明した処理と同様であり、No. 3の処理がユーザデバイスA1510からユーザデバイスB1520へのコンテンツ（セキュアコンテナ）の二次配布において、ユーザデバイスB1520の発行した利用ログB1552に基づいてユーザデバイスA1510が生成した受領ログB1553をサービスプロバイダ240に送付する処理である。

【0202】

サービスプロバイダ240は、ユーザデバイスA1510からユーザデバイスB1520へのコンテンツ（セキュアコンテナ）の二次配布によって生成された受領ログB1553に基づいて、ポイント付加処理（図20のNo. 4の処理）を実行する。

【0203】

サービスプロバイダ240のユーザ管理データベース1534のデータ構成例を図21に示す。各データエントリは、図21に示すようにコンテンツ提供を行なったユーザを示すユーザID、ユーザデバイスID、提供したコンテンツを示すコンテンツID、二次配布に基づく受領ログの識別子としての受領ログID、二次配布に基づくポイントデータが設定されている。

【0204】

サービスプロバイダ240は、これらのデータから、ユーザ毎の集計ポイント、あるいはユーザデバイス毎の集計ポイント等を計数し、例えば所定ポイントに達したユーザ、ユーザデバイスに対して特典を与えることが可能となる。特典としては、例えば、次回のコンテンツ価格を割り引いたり、コンテンツ利用制限を緩和したり、あるいは景品サービスを行なうことなどが可能である。

【0205】

これらのサービスプロバイダによるポイント付加処理と、前述のクリアリングセンタによるコンテンツ利用料金の決済処理は、それぞれに受領ログを送付することによってそれぞれ実行可能であり、いずれか一方のみの処理、または両者の処理を並列に実行することも可能である。

【0206】

〔6. 決済処理の具体例〕

次に、本発明のコンテンツ取り引きシステムにおける具体的な処理例について図を参照して説明する。

【0207】

図22は、クリアリングセンタと、口座管理機関での決済処理の具体例を示している。図22において、ユーザデバイス2210は、サービスプロバイダまたはユーザデバイスB2220からコンテンツを購入する。なお、この例においてコンテンツの利用料金は1000円であるとする。この利用価格、さらに、コンテンツ利用者から徴収した利用料金の配分情報は、コンテンツを格納したセキュアコンテナの価格情報、販売条件に記録されている。

【0208】

まず、ユーザデバイスA2210の電子マネーに対する利用可能な金額の設定処理について説明する。ユーザデバイスA2210を管理する管理ユーザであるユーザAは例えば銀行である口座管理機関2240に100,000円分のユーザAの口座2241を有する。ユーザAの要求により、口座管理機関2240は、電子マネーとして利用可能な金額、10,000円を電子マネーを管理するクリアリングセンタ2230のユーザAの電子マネー口座に振り替える。この処理は、電子マネーの電子データ上での決済処理を実行するクリアリングセンタ2230に通知され、クリアリングセンタ2230は、クリアリングセンタ2230内に設置された各ユーザの電子マネー残高を管理するユーザ残高管理サーバのユーザAの残高を10,000円として設定する。この残高設定の後、この設定金額がユーザデバイスA2210に対して通知される。この通知は、発行ログ2211を生成してユーザデバイスA2210に送信する処理として実行される。なお、この発行ログ送信処理は、相互認証処理、クリアリングセンタの署名処理、ユーザデバイスAによる署名検証等の一連の処理を行なって実行される。

【0209】

この発行ログ2211に設定された残高に相当する金額がユーザデバイスA2210において電子マネーを使用した支払処理で使用可能となる。これは、クリ

アーリングセンタ2230の残高管理データと一致するものとなる。

【0210】

ユーザデバイスA2210は、コンテンツを利用するため電子マネーから1000円を引出して支払うことになる。ユーザデバイスA2210は、この支払い処理を利用ログの生成およびコンテンツ提供者に対する利用ログ送付処理として実行する。また、同時に残高情報から1000を引くため、残高は9,000円になる。コンテンツ提供者は、サービスプロバイダまたはユーザデバイスB2220であり、サービスプロバイダまたはユーザデバイスB2220は、ユーザデバイスAから受信した利用ログに基づいて、受領ログを生成してクリアリングセンタ2230に送付する。

【0211】

クリアリングセンタ2230は、受領ログに記録された配分情報に従って、決済構成を構築し、これを振り替え要求として口座管理機関2240に送信する。ここでの決済処理構成は、コンテンツ受領者（ユーザデバイスA2210）からコンテンツ提供者（サービスプロバイダまたはユーザデバイスB2220）にコンテンツ利用料金1000円を支払う処理とする。

【0212】

口座管理機関2240は、クリアリングセンタ2230から決済処理構成データを受領し、データに従って振替処理を実行する。すなわち、クリアリングセンタの管理するユーザ口座2242からコンテンツ利用料金1000円を引出して、コンテンツ提供者であるサービスプロバイダまたはユーザデバイスB2220の口座2243に1000円を振り替える処理を実行する。

【0213】

これらの一連の処理を実行すると口座管理機関2240は、振替確認をクリアリングセンタ2230に送信する。クリアリングセンタ2230は、振替確認を受信すると、ユーザ残高管理サーバのデータを振り替え処理に応じて更新する。図22では、ユーザAの電子マネー残高を10000円から9000円に設定する。なお、ユーザ残高管理サーバのデータ中、ユーザBの残高は0のままである。これは口座管理機関2240のユーザBの口座は実際の口座であり、電子マネ

ーの残高を示す口座ではないからである。すなわち、クリアリングセンタ口座2242内にユーザBまたはサービスプロバイダの残高がないからである。

【0214】

次に、図23を用いて、ユーザ間でのコンテンツの二次配布（世代間配信または二次配信）により、各ユーザデバイス間でのコンテンツ料金支払いにおいて発生する各ユーザデバイスの電子マネーの残高更新処理例について説明する。

【0215】

図23は、コンテンツプロバイダ2310の制作したコンテンツがコンテンツサービスプロバイダ2320、ユーザデバイスA2330を介してユーザデバイスB2340に流通し、ユーザデバイスB2340が、コンテンツをユーザデバイスC2350に配信して、ユーザデバイスC2350が、ユーザデバイスB2340に利用料金を支払った場合の処理例である。

【0216】

この例において、コンテンツの利用料金は500円であり、コンテンツを格納したセキュアコンテナの価格情報、販売条件には、図23の口座管理機関2370の【利益配分】の欄に示す配分情報が記録されているものとする。すなわち、コンテンツプロバイダに400円、サービスプロバイダに10円、コンテンツ提供ユーザに50円、クリアリングセンタに40円の設定がなされている。

【0217】

図23の(1)～(10)の順に処理が進行する。まず、ユーザデバイスC2350の管理ユーザは、口座管理機関2370のユーザC口座に入金処理（図23の(1)の処理）をするとともに、電子マネーとして利用可能な金額、この場合は10000円を設定するように要求する。口座管理機関2370は、ユーザC口座から10000円をクリアリングセンタ管理口座に振替処理を行ない、これをクリアリングセンタ2360に通知する。クリアリングセンタ2360は、ユーザ管理サーバと、ユーザ残高管理サーバの各データベースにユーザCが10000円の電子マネーを使用可能とする設定を実行し、発行ログをユーザデバイスC2350に発行（図23の(2)の処理）する。

【0218】

ユーザデバイスC2350は、ユーザデバイスB2340からコンテンツ配信を受け（図23の（3）の処理）、電子マネーによる支払いを行なう。この際、電子マネーの残高をコンテンツ利用料金の500円分減少させて、ユーザデバイスCからユーザデバイスBに対するコンテンツの料金支払いであることが記録された利用ログをユーザデバイスB2340に発行（図23の（4）の処理）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【0219】

ユーザデバイスB2340は、ユーザデバイスC2350から受信した利用ログに基づいて、受領ログを生成してクリアリングセンタ2360に送信（図23の（5）の処理）する。この受領ログは利用ログに記録されたデータを含むものであり、ユーザデバイスCからユーザデバイスBに対するコンテンツの料金支払いであること、およびコンテンツ料金配分情報が記録されている

【0220】

クリアリングセンタ2360は、受領ログをユーザ管理サーバのユーザデータと照合して、センタの管理するユーザによる決済要求であることを確認して、決済サーバのコンテンツ料金決済データの更新処理を行ない、コンテンツ料金配分情報に基づく振替構成を構築して、振替構成データを伴う振替要求を口座管理機関2370に送信（図23の（6）の処理）する。

【0221】

口座管理機関2370は、図23の口座管理機関2370の枠内に記載した通りの【利益配分】情報に従ってそれぞれの口座に対する振替処理を実行（図23の（7）の処理）する。図には、ユーザCとユーザBの電子マネー決済についてのみ記載してあるが、口座管理機関2370は、他のコンテンツプロバイダ等の口座に対する振替も実行する。なお、利益配分の情報は、受領ログから抽出してクリアリングセンタ2360から口座管理機関2370へ送信するようにしてもよい。

【0222】

口座管理機関2370による振替処理が終了すると、振替確認がクリアリング

センタ2360に通知（図23の（8）の処理）され、クリアリングセンタ2360は、自身が管理する電子マネー情報の決済処理、すなわち各ユーザ電子マネー残高の更新処理を実行（図23の（9）の処理）する。さらに、コンテンツを提供したユーザデバイス2340に対してコンテンツの利益配分情報に従った50円の発行（図23の（10）の処理）を行なう。

【0223】

なお、一連の処理において、データ通信を実行する各手段は、それぞれ相互認証処理、送信データに対する署名処理、受信データに対する署名確認処理を行なっている。このような一連の処理により、コンテンツのユーザ間における配信において、予めセキュアコンテナに設定された利益配分情報に従った決済処理が実行されることになる。

【0224】

上述の図23の例では、受領ユーザデバイスC、2350にコンテンツを二次配布したユーザデバイス2340が生成した受領ログを直接クリアリングセンタ2360に送付する例を示したが、ユーザ間でコンテンツの二次配布（世代間配信または二次配信）を行なったユーザデバイスがクリアリングセンタではなく、サービスプロバイダに受領ログを送付する例を図24に示す。ユーザデバイスがクリアリングセンタではなく、サービスプロバイダに受領ログを送付することにより、サービスプロバイダにおいて、利益分配処理、ポイント付与の管理等コンテンツ流通に伴う各種の処理を一括して実行することが可能となり、また、クリアリングセンタは電子マネーの発行（発行ログの管理）と受領ログに基づく精算業務のみを実行する構成とすることができます。

【0225】

図24に示す処理構成について説明する。図24の（1）～（22）の順に処理が進行する。図24では、ユーザデバイスA2410から、ユーザデバイスB2420にコンテンツが二次配布（世代間配信または二次配信）された例である。まず、ユーザデバイスB2420がユーザデバイスA2410にコンテンツを要求（1）する。次に、ユーザデバイスA2410はコンテンツ（セキュアコンテナ）をユーザデバイスB2420に送信（2）する。ユーザデバイスB242

0は、販売条件等を確認して購入処理を実行し、電子マネーによる支払を行なう。この際、電子マネーの残高情報はコンテンツの利用金額に応じて減額（¥20,000→¥19,500）（3）される。さらにユーザデバイスB2420は、コンテンツの料金支払いであることが記録された利用ログを生成してユーザデバイスAに送付（4）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【0226】

ユーザデバイスA2410は、利用ログの署名検証（5）を実行し、利用ログに基づく受領ログを生成して保存（6）し、コンテンツ鍵をユーザデバイスB2420に送信（7）する。受領ログは利用ログに記録されたデータを含むものであり、ユーザデバイスCからユーザデバイスBに対するコンテンツの料金支払いであること、およびコンテンツ料金配分情報が記録されている。ユーザデバイスA2410は、生成した受領ログをサービスプロバイダ2430に送信（8）する。

【0227】

受領ログを受信したサービスプロバイダ2430は、受領ログの署名を検証して受領ログに記録された利益分配情報、ポイント付与情報に従った処理を実行して、処理データをユーザ管理データベースあるいは利益分配管理サーバに格納する。これらの一連の処理が終了すると、サービスプロバイダ2430は受領ログをクリアリングセンタ2440に転送（10）する。

【0228】

クリアリングセンタ2440は、受領ログをユーザ管理サーバのユーザデータと照合して、センタの管理するユーザによる決済要求であることを確認して、決済サーバのコンテンツ料金決済データの更新処理を行ない、コンテンツ料金のクリアリングセンタ管理口座からサービスプロバイダの口座への振替要求を口座管理機関2450に送信（11）する。

【0229】

口座管理機関2450は、クリアリングセンタ2440からの振替要求に基づいてクリアリングセンタ管理口座2451からサービスプロバイダ管理口座24

52への振替を実行（12）する。この例では、利益配分情報に基づく利益配分処理は、サービスプロバイダが管理するので、クリアリングセンタ2440からの振替要求に基づく処理は、クリアリングセンタ管理口座2451からサービスプロバイダ管理口座2452への振替処理のみとなる。すなわち、図に示すようにクリアリングセンタ管理口座2451が、¥30,000から¥29,500に変更され、サービスプロバイダの口座2452が¥0から¥500に変更される。口座管理機関2450の振替が終了すると、口座管理機関2450はクリアリングセンタ2440に振替確認を送信（13）し、クリアリングセンタ2440は、振替確認に基づいて電子マネー残高管理サーバ内のユーザデバイスB2420の管理ユーザであるユーザBの残高データの更新（14）を行なう（ユーザBの残高が¥20,000から¥19,500に変更される）。この更新により、ユーザデバイスB2420の電子マネー残高（¥19,500）と一致する残高がクリアリングセンタ2440の電子マネー残高管理サーバ内のユーザBの残高データ（¥19,500）に記録される。

【0230】

次にクリアリングセンタ2440は、サービスプロバイダ2430にユーザデバイスB2420からのコンテンツ料金の支払い処理が終了したことを報告（15）する。サービスプロバイダ2430は、クリアリングセンタ2440からの報告を受けると、先に受領ログに基づいて決定されている利益配分情報に基づく振替依頼を口座管理機関2450に送信（16）する。口座管理機関2450は、サービスプロバイダ2430からの配分情報に従ってそれぞれの口座に対する振替処理を実行（17）する。図24に示す例では、コンテンツプロバイダの口座2453と、クリアリングセンタの口座2454にそれぞれ利益配分情報に従った金額の振替がなされている。すなわち、振替処理により、クリアリングセンタ管理口座2451が¥29,500→¥29,550、サービスプロバイダの管理口座2452が、¥500→¥10、コンテンツプロバイダの口座2453が、¥0→¥400、クリアリングセンタの口座2454が、¥0→¥40に変更される。

【0231】

口座管理機関2450によるこれらの振替が終了すると、口座管理機関2450は、配分処理の終了を示す振替確認をクリアリングセンタ2440に送信（19）する。クリアリングセンタ2440は、振替確認を受領すると、クリアリングセンタ2440の管理するユーザデバイスAの電子マネーの残高変更処理（ユーザAの残高を¥10,000から¥10,050に変更）を実行（20）する。この処理は、先にサービスプロバイダ2430から受領した受領ログに基づく処理、すなわち二次配布による利益配分（図の例では¥50）がユーザデバイスA2410の管理ユーザであるユーザAに渡される処理となる。クリアリングセンタ2440によるユーザデバイスAの電子マネーの残高変更処理が終了すると、ユーザデバイスAに対して利益配分（¥50）の発行金額を有する新たな発行ログを送信（21）し、ユーザデバイスA2410は発行ログに基づいて電子マネーの残高を変更（22）（残高を¥10,000から¥10,050に変更）する。

【0232】

なお、図の（21）で送付する発行ログは、前述した発行ログの追加発行処理と同様の処理として、すでにユーザデバイスA2410に対して発行済みの「発行ロガーo1d」と電子マネー残高データの送信をクリアリングセンタ2440側から要求し、ユーザAに対する利益額と、ユーザから受信した「発行ロガーo1d」に基づく電子マネー使用可能残高との合計を新たな発行ログである「発行ロガーネw」の発行金額として設定して新たな発行ログ「発行ロガーネw」をユーザデバイスAに送信する構成としてもよい。この場合、「発行ロガーo1d」はクリアリングセンタ2440において無効化される。

【0233】

次に、図25を用いて、各種ログを用いたコンテンツ配信における決済処理の処理例について説明する。図25はコンテンツ流通における決済処理の管理の中心がサービスプロバイダであるローカル管理方式の例である。

【0234】

図25に示す番号（1）～（18）の順に処理が進行する。この例では、サービスプロバイダ2520からユーザデバイスA2510がコンテンツを購入する

場合の処理例である。

【0235】

まず、ユーザデバイスA2510は、電子マネーによる支払処理を可能とするため、クリアリングセンタ2530のユーザ管理サーバへの登録および電子マネー残高管理サーバの残高を設定する処理をクリアリングセンタ2530に対して入金命令（1）として要求する（電子マネー：¥0→¥10,000）。クリアリングセンタ2530は要求に従って口座管理機関2540に対してユーザAの口座2541からクリアリングセンタ管理口座2542への振替を要求し、口座管理機関2540は要求に従って振り替え処理を実行（2）する（ユーザAの口座2541：¥10,000→¥90,000、クリアリングセンタの口座2542：¥0→¥10,000）。振替処理が終了すると確認応答がクリアリングセンタ2530に対してなされ、応答に応じて、クリアリングセンタ2530は、電子マネー残高管理サーバのユーザAの残高を入金処理金額に応じて更新（3）（ユーザA2510の電子マネー：¥0→¥10,000）し、その金額を発行金額として設定した発行ログをユーザデバイスA2510に送信（4）する。

【0236】

次に、ユーザデバイスA2510は、サービスプロバイダ2520にコンテンツを要求（5）する。次に、サービスプロバイダ2520はコンテンツ（セキュアコンテナ）をユーザデバイスA2510に送信（6）する。ユーザデバイスA2510は、販売条件等を確認して購入処理を実行し、電子マネーによる支払い処理としての電子マネー残高変更（7）を実行（¥10,000→¥9,500）し、コンテンツの料金支払いであることが記録された利用ログを生成してサービスプロバイダ2520に送付（8）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【0237】

サービスプロバイダ2520は、利用ログの署名検証を実行（9）し、利用ログに基づくコンテンツ料金配分情報を取得して、受領ログを生成・保存（10）して、コンテンツ鍵をユーザデバイスA2510に送信（11）する。その後、決済時に受領ログをクリアリングセンタ2530に送信（12）する。

【0238】

クリアリングセンタ2530は、受領ログの格納データとユーザ管理サーバのユーザデータとの照合処理を実行して、センタの管理するユーザによる決済要求であることを確認して、コンテンツ料金のクリアリングセンタ管理口座からサービスプロバイダの口座への振替要求を口座管理機関2540に送信（13）する。

【0239】

口座管理機関2540は、クリアリングセンタ2530からの振替要求に基づいてクリアリングセンタ管理口座2542からサービスプロバイダ管理口座2543への振替を実行（14）する（サービスプロバイダ管理口座2543：¥0→¥500）。この例では、利益配分情報に基づく利益配分処理は、サービスプロバイダ2520が管理するので、クリアリングセンタ2530からの振替要求に基づく処理は、クリアリングセンタ管理口座2542からサービスプロバイダ管理口座2543への振替処理のみとなる。口座管理機関2540の振替が終了すると、口座管理機関2540はクリアリングセンタ2530に振替確認を送信（15）し、クリアリングセンタ2530は、振替確認に基づいて電子マネー残高管理サーバ内のユーザA（ユーザデバイスA2510の管理ユーザ）の残高データの更新（16）（¥10,000→¥9,500）を行なう。

【0240】

次にクリアリングセンタ2530は、サービスプロバイダ2520にユーザデバイスA2510からのコンテンツ料金の支払い処理が終了したことを振替確認として報告（17）する。サービスプロバイダ2520は、クリアリングセンタ2530からの報告を受けると、先に利用ログに基づいて決定されている利益配分情報に基づく振替依頼を口座管理機関2540に送信する。口座管理機関2540は、サービスプロバイダ2520からの配分情報に従ってそれぞれの口座に対する振替処理を実行（18）する。図25に示す例では、コンテンツプロバイダの口座2544と、クリアリングセンタの口座2545にそれぞれ利益配分情報に従った金額の振替がなされている。すなわち、サービスプロバイダ管理口座2543：¥500→¥60、コンテンツプロバイダの口座2544：¥0→¥

400、クリアリングセンタの口座2545：¥0→¥40の振替がなされる。

【0241】

この図25の例は、サービスプロバイダが利益分配、ポイント管理等のコンテンツ流通に伴う各処理を実行し、クリアリングセンタは電子マネーの残高管理が主業務となる。

【0242】

次に、図26を用いて、ユーザデバイスにおいて残高管理を実行せず、クリアリングセンタが電子マネーの残高管理を行なうクリアリングセンタ管理方式の処理例を説明する。（1）～（15）の順に処理が進行する。この例では、サービスプロバイダ2620からユーザデバイスA2610がコンテンツを購入する場合の処理例である。

【0243】

まず、ユーザデバイスA2610は、電子マネーによる支払処理を可能とするため、クリアリングセンタ2630のユーザ管理サーバへの登録および電子マネー残高管理サーバの残高を設定する処理をクリアリングセンタ2630に対して入金命令（1）として要求する。クリアリングセンタ2630は要求に従って口座管理機関2640に対してユーザデバイスA2610の管理ユーザであるユーザAの口座2641からクリアリングセンタ管理口座2642への振替を要求し、口座管理機関2640は要求に従って振り替え処理を実行（2）する。すなわち、ユーザAの口座2641：¥100,000→¥90,000、クリアリングセンタ管理口座2642：¥0→¥10,000の振替が実行される。振替処理が終了すると確認応答がクリアリングセンタ2630に対してなされ。応答に応じて、クリアリングセンタ2630は、電子マネー残高管理サーバのユーザAの残高を入金処理金額に応じて更新（3）（¥0→¥10,000）する。

【0244】

このセンタ管理方式では、ユーザデバイスA2610は、クリアリングセンタ2630に入金命令を送信とともにサービスプロバイダ2620にコンテンツを要求（4）することができる。先の図25の例では、ユーザデバイス側において電子マネーの残高チェックを実行シテコンテンツの購入処理を実行していたが

、本例では、クリアリングセンタ側で電子マネー残高を更新して、その報告を受けたサービスプロバイダ2620が、その報告後、ユーザデバイスAに対してコンテンツ鍵を送信する方式となっている。

【0245】

ユーザデバイスA2610がサービスプロバイダ2620にコンテンツを要求すると、サービスプロバイダ2620はコンテンツ（セキュアコンテナ）をユーザデバイスA2610に送信（5）する。ユーザデバイスA2610は、販売条件等を確認して購入処理を実行し、電子マネーによる支払い、コンテンツの料金支払いであることが記録された利用ログを生成してサービスプロバイダ2620に送付（6）する。この際に生成される利用ログには、セキュアコンテナに記録された配分情報が記録されている。

【0246】

サービスプロバイダ2620は、利用ログの署名検証を実行し、利用ログに基づくコンテンツ料金配分情報を取得して、受領ログを生成してクリアリングセンタ2630に送信（7）する。

【0247】

クリアリングセンタ2630は、受領ログをユーザ管理サーバのユーザデータと照合して、センタの管理するユーザによる決済要求であることを確認して、決済サーバのコンテンツ料金決済データの更新処理を行ない、電子マネー残高管理サーバの残高確認（8）を行い、コンテンツ料金のクリアリングセンタ管理口座からサービスプロバイダの口座への振替要求を口座管理機関2640に送信（9）する。

【0248】

口座管理機関2640は、クリアリングセンタ2630からの振替要求に基づいてクリアリングセンタ管理口座2642からサービスプロバイダ管理口座2643への振替を実行（10）する（クリアリングセンタ管理口座2642：¥10,000→¥9,500、サービスプロバイダ管理口座2643：¥0→¥500）。この例においても、利益配分情報に基づく利益配分処理は、サービスプロバイダ2620が管理するので、クリアリングセンタ2630からの振替要求

に基づく処理は、クリアリングセンタ管理口座2642からサービスプロバイダの口座2643への振替処理のみとなる。口座管理機関2640の振替が終了すると、口座管理機関2640はクリアリングセンタ2630に振替確認を送信（11）し、クリアリングセンタ2630は、振替確認に基づいて電子マネー残高管理サーバ内のユーザAの残高データの更新（¥10,000→¥9,500）（12）を行なう。

【0249】

次にクリアリングセンタ2630は、サービスプロバイダ2620にユーザデバイスA2610からのコンテンツ料金の支払い処理が終了したことを振替確認送信（13）する。サービスプロバイダ2620は、クリアリングセンタ2630からの振替確認を受けると、コンテンツ鍵をユーザデバイスA2610に送信（14）する。さらに、サービスプロバイダ2620は、先に利用ログに基づいて決定されている利益配分情報に基づく振替依頼を口座管理機関2640に送信する。口座管理機関2640は、サービスプロバイダ2620からの配分情報に従ってそれぞれの口座に対する振替処理を実行（15）する。図26に示す例では、コンテンツプロバイダの口座2644と、クリアリングセンタの口座2645にそれぞれ利益配分情報に従った金額の振替がなされている。すなわち、サービスプロバイダの口座2643：¥500→¥60、コンテンツプロバイダの口座2644：¥0→¥400、クリアリングセンタの口座2645：¥0→¥40の各振替がなされる。

【0250】

本例においては、ユーザデバイスA2610は、電子マネーの残高確認が不要であり、クリアリングセンタ2630において、電子マネー残高管理サーバ内のユーザ残高が確認され、口座管理機関2640において、ユーザAからのコンテンツ利用料金振替が行なわれて、クリアリングセンタ2630内で管理する電子マネー残高の更新がなされ、これらの処理が完結したことをサービスプロバイダ2620に報告されて始めて、コンテンツ鍵がユーザデバイスA2610に送信されることになる。この処理構成によれば、クリアリングセンタ2630において未決済分のコンテンツ料金の発生を防止することができる。なお、手数料を減

らすため、実際の振替処理は一括して行ない、クリアリングセンタ2630内のデータのみ変更して後に振替処理を行なう構成としてもよい。

【0251】

[7. ログを利用したユーザ管理]

先に説明したように、本発明のコンテンツ取り引きシステムおよびコンテンツ取り引き方法においては、発行ログ、利用ログ、受領ログ等が各デバイス、機関において流通することになる。各ログには図6で説明したように、様々な情報が格納されている。ここでは、これらの情報を利用したユーザ管理構成について説明する。

【0252】

(7-1) ユーザの利用料金の管理

図6を用いて説明した各ログの構成において明らかなように、コンテンツを購入しようとするユーザが生成してサービスプロバイダに対して送信する利用ログには、利用金額が情報として格納されている。ここでは、この利用ログに記録される利用金額情報をを利用して高額な料金の支払をチェックする構成を説明する。

【0253】

図27に利用料金チェック処理フローを示す。図27のフローにしたがって説明する。ステップS2701において、ユーザが生成した利用ログがサービスプロバイダに送信される。ステップS2702において、サービスプロバイダは受領した利用ログ中の利用金額を確認し、予め定めた閾値との比較処理を実行する。この閾値は、例えばすべてのユーザに対して共通の閾値でもよいし、あるいはユーザの年齢、利用状況等に基づいてサービスプロバイダが独自に設定した閾値でもよい。サービスプロバイダはこれらの閾値を設定したユーザ管理用のデータを保有する。

【0254】

ステップS2703において要検査の判定がなされると、サービスプロバイダは、ステップS2704において利用ログから発行ログを取り出して、取り出した発行ログをクリアリングセンタに送信する。ステップS2705において、クリアリングセンタは、サービスプロバイダから受領した発行ログに基づいて、ク

リアリングセンタ内の電子マネー残高管理サーバのユーザ残高をチェックし、ステップS2706においてクリアリングセンタは残高チェックデータをサービスプロバイダに送信する。サービプロバイダはチェックデータに基づいて問題なし（ステップS2707においてYes）と判定された場合は、正当なコンテンツ購入処理と判定し、ユーザデバイスに対するコンテンツ鍵送信等の通常処理（ステップS2708）に移行する。一方、コンテンツ利用料金の回収が困難になるおそれがある等、問題あり（ステップS2707においてNo）と判定された場合は、ユーザデバイスに対してコンテンツ購入の拒否応答を行ないコンテンツ鍵の送信を中止（ステップS2709）する。

【0255】

この処理により、コンテンツの不正取引、あるいは未成年者による高額商品の取引等を未然に防止することが可能となる。なお、これらの利用金額チェックはクリアリングセンタがみずから実行する構成として、問題ありと判定された場合にクリアリングセンタからサービスプロバイダに例えばユーザ照会処理を実行するように要求する構成としてもよい。

【0256】

さらに、ユーザデバイス側において、ユーザデバイス固有の利用金額上限値としての閾値を設定し、設定した閾値データをメモリに格納し、コンテンツ利用に伴う利用ログの生成の際に閾値データを参照して、利用ログに閾値を超える利用金額が設定される場合は、閾値を超える利用料金の設定であることまたはクリアリングセンタによるチェック処理が必要であることを示す識別データ（識別ビット）を利用ログに付加する構成としてもよい。識別データが付加された利用ログを受領したサービスプロバイダは、識別データに基づいてクリアリングセンタに対するユーザの残高チェック処理を要求する。本構成によれば、サービスプロバイダ側でユーザの閾値データを保有する必要がなく、さらにユーザ毎に任意の閾値を設定することが可能となる。

【0257】

（7-2）発行ログの利用期限管理

前述の本発明の説明から明らかなようにコンテンツを購入しようとするユーザ

は、クリアリングセンタから発行ログを受領する。発行ログには図6に示したように、有効期限が設定されている。ここでは、この有効期限に基づく管理について説明する。

【0258】

クリアリングセンタは、ユーザ管理サーバに発行ログを発行したユーザとその発行ログ情報を対応付けたデータを保有している。発行ログには発行金額、有効期限が設定され、発行ログを受領したユーザデバイスは、その発行ログに設定された金額および有効期限内で発行ログに基づいて電子マネーによる支払い処理が可能となる。

【0259】

クリアリングセンタでは、例えば未成年者には小額の発行金額を上限として設定したり、取り引き回数に応じて高額の発行金額を設定する等、ユーザの信用度に基づく発行金額の設定を行なうことができる。さらに、高額な発行金額を設定した発行ログは有効期限を長く設定し、低額の発行金額を設定した発行ログは有効期限を短くする等、各発行ログに応じた有効期限設定が可能となる。

【0260】

クリアリングセンタは、ユーザ管理サーバにおいてすべての発行ログ情報を管理しているとともに、電子マネー残高管理サーバにおいて各ユーザの電子マネー残高を管理しているので、クリアリングセンタは、これらの各データに基づいて定期的な監査処理を実行し、有効期限の迫った発行ログを有するユーザに対して、発行ログの有効期限を更新した新たな発行ログの発行要求を促すメッセージを送信する等の処理が可能となる。

【0261】

クリアリングセンタによる発行ログの有効期限管理処理のフローを図28に示す。ステップS2801において、クリアリングセンタは、ユーザ管理サーバ、電子マネー残高管理サーバとのデータチェックを実行し、ユーザ管理サーバの格納データに基づいて有効期限が迫っている発行ログを抽出する。このチェック処理は、例えば1ヶ月毎に定期的に実行して、残り有効期限が2ヶ月以内である発行ログを検索する処理として設定する。

【0262】

クリアリングセンタは抽出された発行ログに基づいて発行ログ情報に記録されたユーザデバイス識別子に基づいてユーザデバイスを特定（ステップS2802）し、そのユーザデバイスに対して有効期限の迫った発行ログがあることを示すメッセージを送信（ステップS2803）する。ユーザデバイスは、メッセージを受信し、発行ログの更新要求を実行する（ステップS2804でYes）と、クリアリングセンタは更新要求に基づいて、新たな有効期限を持つ更新された発行ログを生成してユーザデバイスに送信（ステップS2805、S2806）する。ユーザデバイスが、メッセージを受信後、有効期間内に発行ログの更新要求を実行しない（ステップS2804でNo）場合は、有効期間経過後、発行ログの利用期間が経過したことと再発行処理が必要であることを知らせるメッセージをユーザデバイスに送信（ステップS2807）し、クリアリングセンタは、その後のユーザデバイスからの再発行要求があった場合（ステップS2808でYes）は要求に基づいて発行ログの再発行処理を行ない（ステップS2809）、再発行ログをユーザデバイスに送信（ステップS2810）する。

【0263】

このように、クリアリングセンタによって発行ログの管理を行なう構成とすることにより、不正な発行ログの流通、使用を防止することができる。さらに、発行ログの有効期限チェックの際に、クリアリングセンタ電子マネー残高管理サーバの残高を併せてチェックすることにより、利用、回収済みの電子マネー金額と未回収分の電子マネーの集計が可能となる。

【0264】

また、クリアリングセンタは、電子マネー残高管理サーバの定期的なチェックを実行して、電子マネー残高が小額となったユーザデバイスに対して、その旨のメッセージを送信したり、あるいは、残金額をデータとして送信するように構成してもよい。

【0265】

さらに、ユーザデバイス側において、電子マネーの利用時に発行ログの有効期限のチェック処理を実行し、有効期限が過ぎていた場合には、利用ログの生成処

理前にクリアリングセンタに対して発行ログの更新あるいは再発行処理の要求を実行して新たな発行ログの取得を行い、その後に新たな有効期限の設定された新規発行ログに基づく利用ログの生成処理を実行する構成としてもよい。

【0266】

なお、一連の処理において、データ通信を実行するユーザデバイス、クリアリングセンタ、サービスプロバイダ各手段は、それぞれ相互認証処理、送信データに対する署名処理、受信データに対する署名確認処理を行ない、不正なデータ流出が行われない構成とする。

【0267】

以上、特定の実施例を参考しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参照すべきである。

【0268】

【発明の効果】

上述したように、本発明のコンテンツ二次配信制限システムおよびコンテンツ二次配信制限方法に従えば、コンテンツのユーザデバイス間での流通、特に、ユーザデバイスAからユーザデバイスB、ユーザデバイスC、ユーザデバイスDへのコンテンツ配信のように並列的にコンテンツを異なるユーザデバイスに対して配信するコンテンツ二次配信の処理回数に制限を付加することが可能となり、同一のコンテンツの利用毎の管理が可能となり、コンテンツの不正流通が氾濫することなく、コンテンツ提供者、またはサービス提供者の利益が確保されることになる。

【図面の簡単な説明】

【図1】

従来の超流通システムの構成を説明するブロック図である。

【図2】

本発明のコンテンツ取り引きシステムのシステム概要を説明するブロック図で

ある。

【図3】

本発明のコンテンツ取り引きシステムにおいてユーザデバイスの構成例を示す
ブロック図である。

【図4】

本発明のコンテンツ取り引きシステムにおけるコンテンツの流通、ログ情報の
流通形態について説明するブロック図である。

【図5】

本発明のコンテンツ取り引きシステムにおける相互認証処理において使用され
る公開鍵証明書の構成について説明する図である。

【図6】

本発明のコンテンツ取り引きシステムにおいて使用される発行ログ、利用ログ
、受領ログ構成を説明する図である。

【図7】

本発明のコンテンツ取り引きシステムにおいて適用可能な署名生成処理につい
て説明する図である。

【図8】

本発明のコンテンツ取り引きシステムにおいて適用可能な署名生成処理につい
て説明する図である。

【図9】

本発明のコンテンツ取り引きシステムにおいて適用可能な署名検証処理につい
て説明する図である。

【図10】

本発明のコンテンツ取り引きシステムにおいて適用可能な相互認証処理につい
て説明する図である。

【図11】

本発明のコンテンツ取り引きシステムにおいて適用可能な相互認証処理につい
て説明する図である。

【図12】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通において使用されるセキュアコンテナの構成を説明する図である。

【図13】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナに含まれる販売条件情報（UCP）について説明する図である。

【図14】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナに含まれる価格情報について説明する図である。

【図15】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナの流通とログ情報に基づく決済処理構成を説明する図である。

【図16】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナの流通において、ユーザデバイスに記録される使用制御情報（UCS）について説明する図である。

【図17】

本発明のコンテンツ取り引きシステムにおいて発行される受領ログに含まれる受領情報の構成例を説明する図である。

【図18】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバイス間での流通における処理を説明する図である。

【図19】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバイス間での流通における処理フローを説明する図である。

【図20】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバイス間での流通におけるポイント付加処理を説明する図である。

【図21】

本発明のコンテンツ取り引きシステムにおけるセキュアコンテナのユーザデバ

イス間での流通におけるポイント付加処理に使用されるデータベース構成例を説明する図である。

【図22】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通による決済処理の具体例を説明する図である。

【図23】

本発明のコンテンツ取り引きシステムにおけるユーザデバイス間のコンテンツ流通による決済処理の具体例（その1）を説明する図である。

【図24】

本発明のコンテンツ取り引きシステムにおけるユーザデバイス間のコンテンツ流通による決済処理の具体例（その2）を説明する図である。

【図25】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通による決済処理の具体例（ローカル管理方式）を説明する図である。

【図26】

本発明のコンテンツ取り引きシステムにおけるコンテンツ流通による決済処理の具体例（クリアリングセンタ管理方式）を説明する図である。

【図27】

本発明のコンテンツ取り引きシステムにおける利用ログの利用金額による決済管理処理フローを説明する図である。

【図28】

本発明のコンテンツ取り引きシステムにおける発行ログの有効期限による発行ログ管理フローを説明する図である。

【符号の説明】

220 ユーザデバイス

221 電子マネー

222 発行ログ

240 サービスプロバイダ

251 発行ログ

252 利用ログ
253 受領ログ
260 クリアリングセンタ
280 口座管理機関
281 ユーザ口座
282 サービスプロバイダ口座
283 クリアリングセンタ管理口座
300 ユーザデバイス
301 制御部
302 暗号処理部
303 記録デバイスコントローラ
304 読み取り部
305 通信部
306 制御部
307 内部メモリ
308 暗号／復号化部
310 電子マネー¹
311 制御部
312 暗号処理部
313 メモリ
321 メインC P U
322 R A M
323 R O M
324 入力インタフェース
326 P I O
327 S I O
350 記録デバイス
351 暗号処理部
352 外部メモリ

360 メディア
370 通信手段
410 公開鍵証明書発行局（IA）
1200 セキュアコンテナ
1201 コンテンツ
1202 價格情報
1203 販売情報（UCP）
1204 電子署名
1301 UCP世代管理情報
1302 二次配信可能回数
1510 ユーザデバイスA
1520 ユーザデバイスB
1511, 1521 電子マネー¹
1531 発行ログA
1532 利用ログA
1533 受領ログA
1551 発行ログB
1552 利用ログB
1553 受領ログB
1570 ユーザデバイスC
1601 UCS世代管理情報
1701 配分情報
1702 UCP世代管理情報
1810 サービスプロバイダ
1811 制御部
1812 コンテンツデータベース
1813 ユーザ情報データベース
1814 暗号処理部
1815 通信部

1820 ユーザデバイスA
1830 ユーザデバイスB
1821, 1831 制御部
1822, 1832 暗号処理部
1824, 1834 メモリ
1825, 1835 記憶部
1826, 1836 データ再生部
1827, 1837 通信部
1828, 1838 電子マネー^一
1840 クリアリングセンタ
1841 制御部
1842 データベース
1844 暗号処理部
1845 通信部
2210 ユーザデバイスA
2211 発行ログ
2220 サービスプロバイダまたはユーザデバイスB
2230 クリアリングセンタ
2240 口座管理機関
2241 ユーザA口座
2242 クリアリングセンタ口座
2243 サービスプロバイダ、ユーザB口座
2310 コンテンツプロバイダ
2320 サービスプロバイダ
2330 ユーザデバイスA
2340 ユーザデバイスB
2350 ユーザデバイスC
2360 クリアリングセンタ
2370 口座管理機関

2410, 2420, 2510, 2610 ユーザデバイス

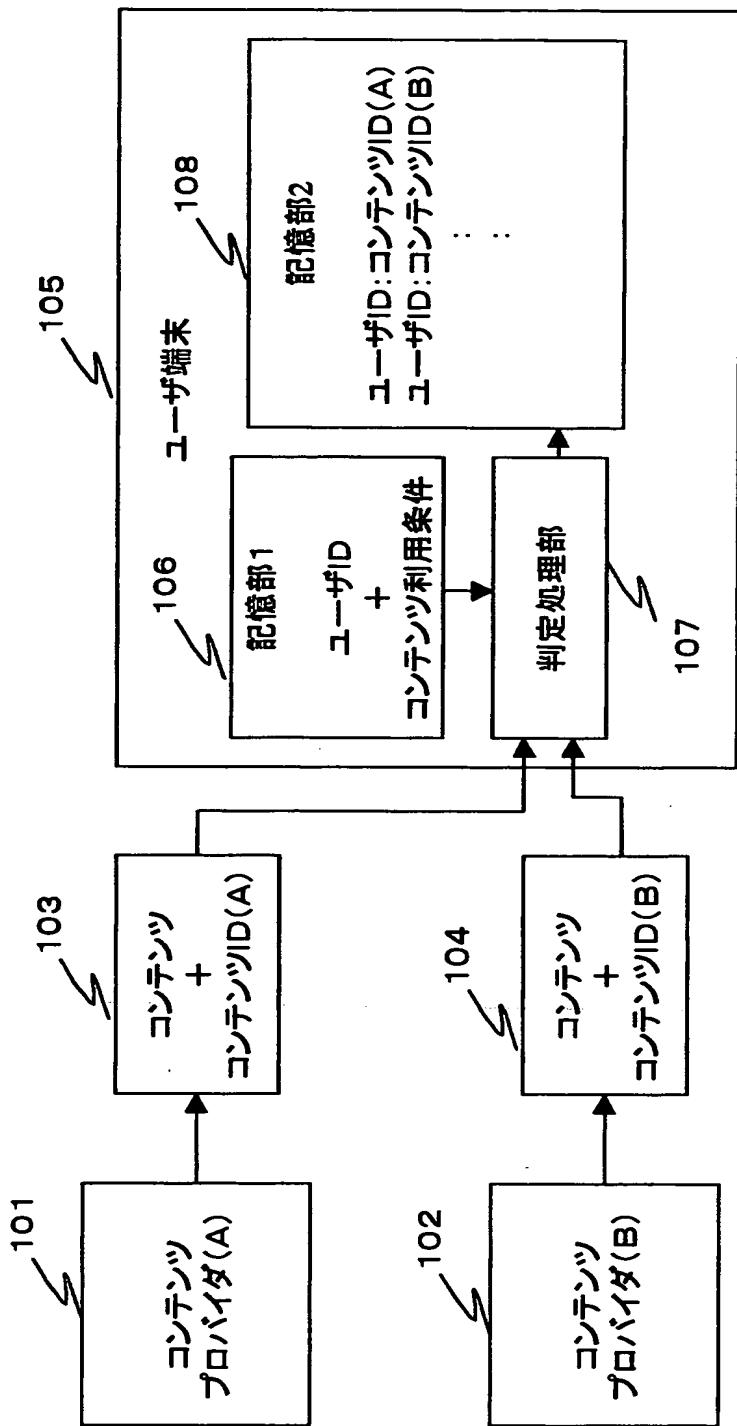
2430, 2520, 2620 サービスプロバイダ

2440, 2530, 2630 クリアリングセンタ

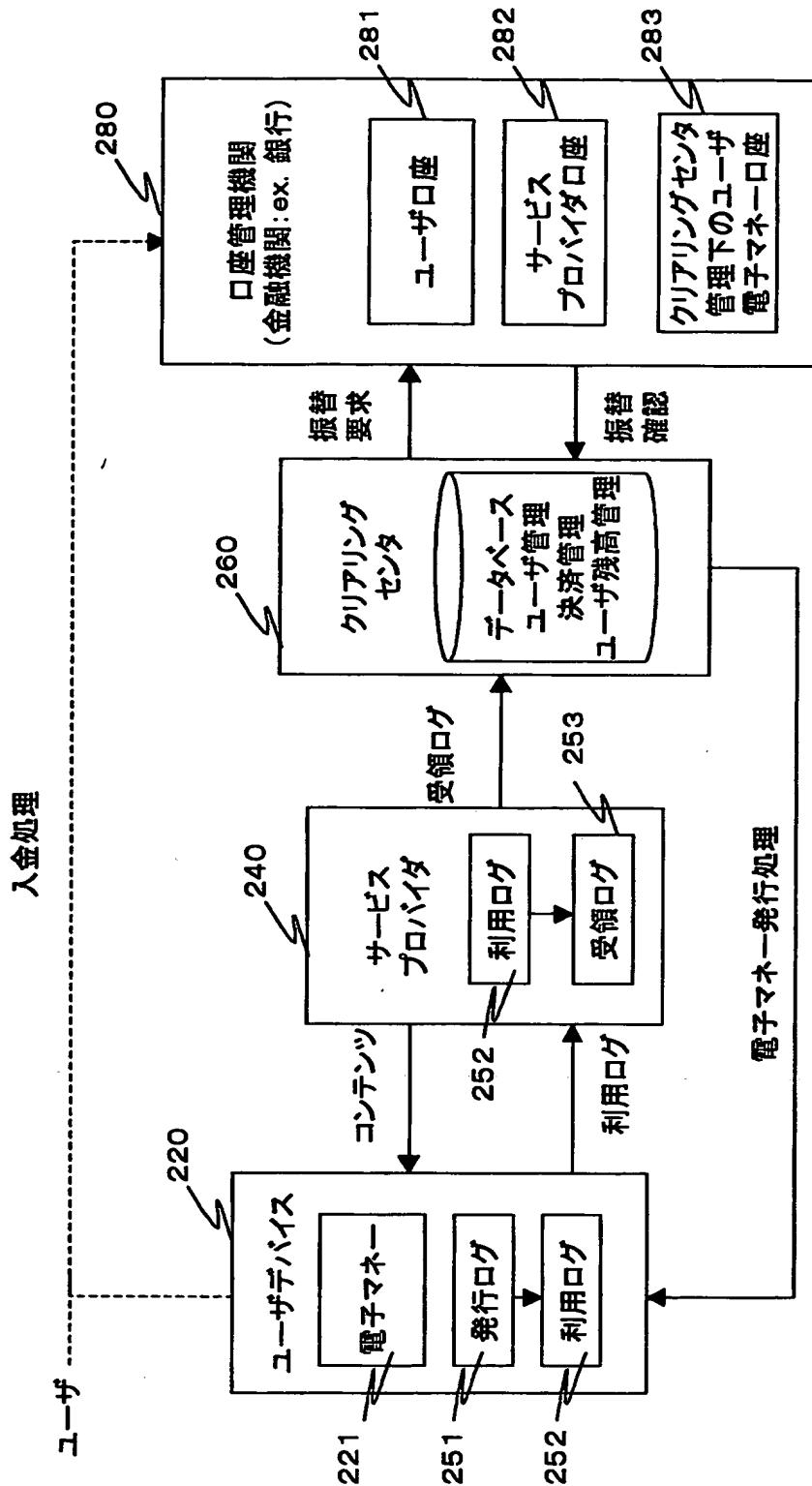
2450, 2540, 2640 口座管理機関

【書類名】 図面

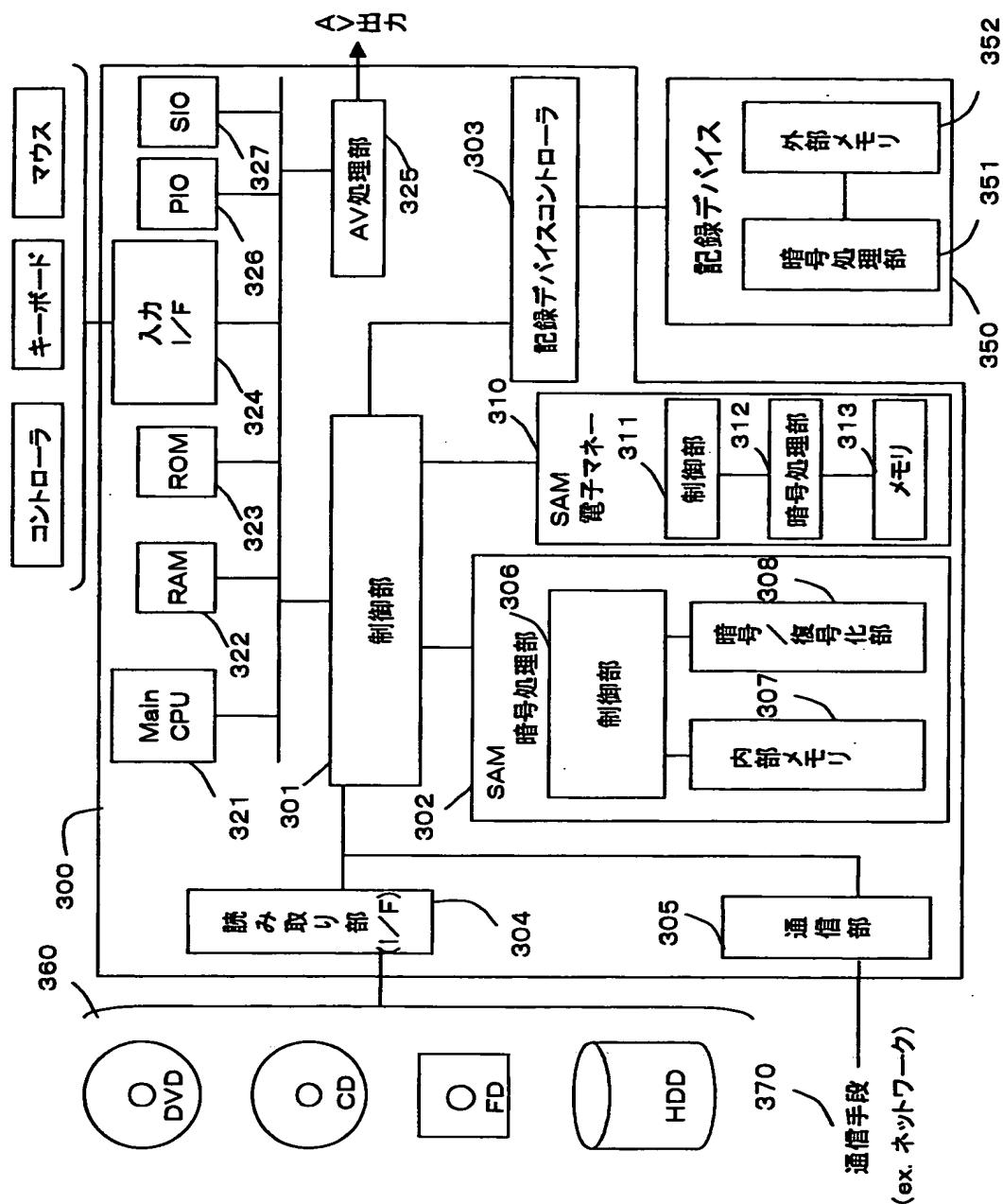
【図1】



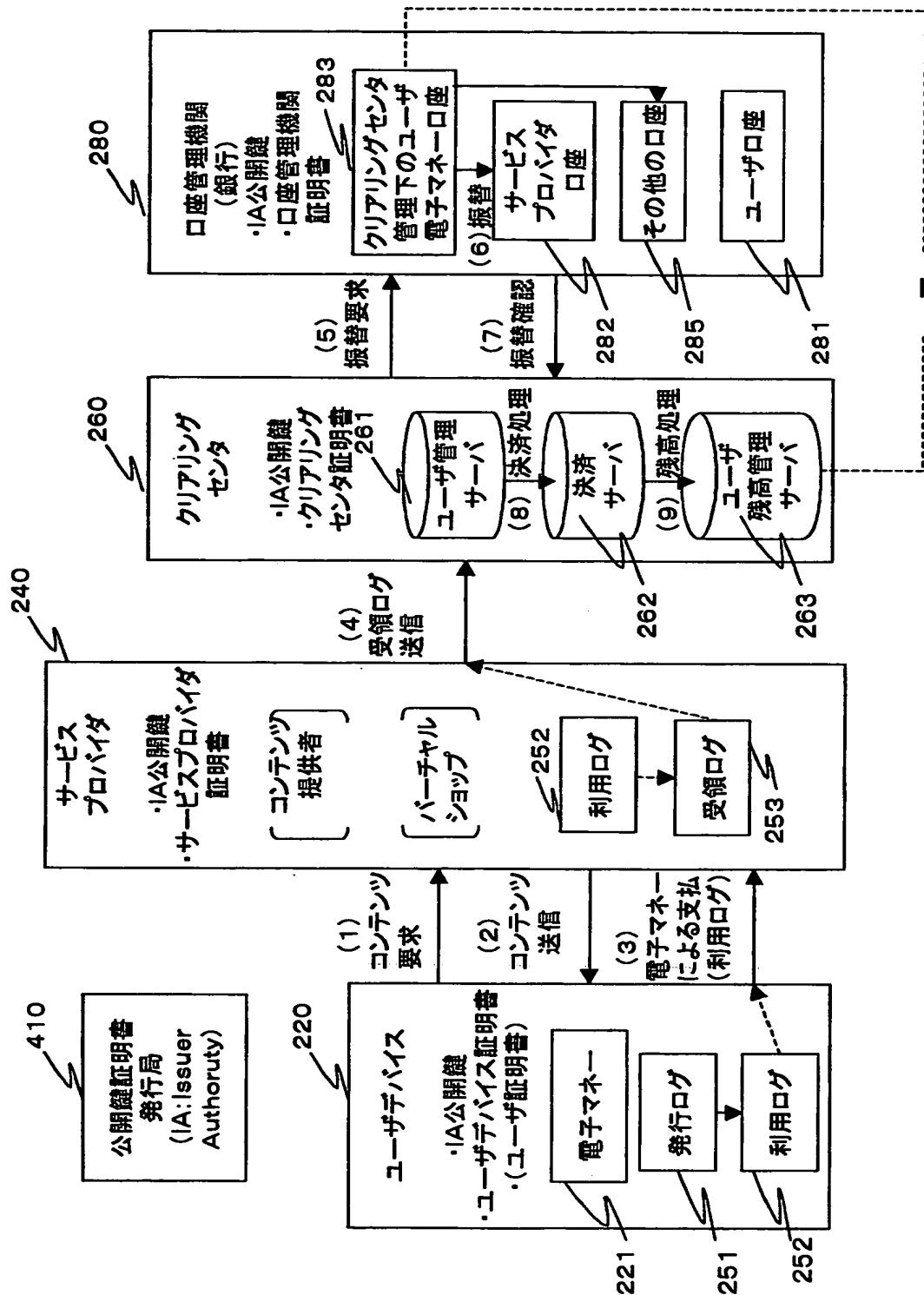
【図2】



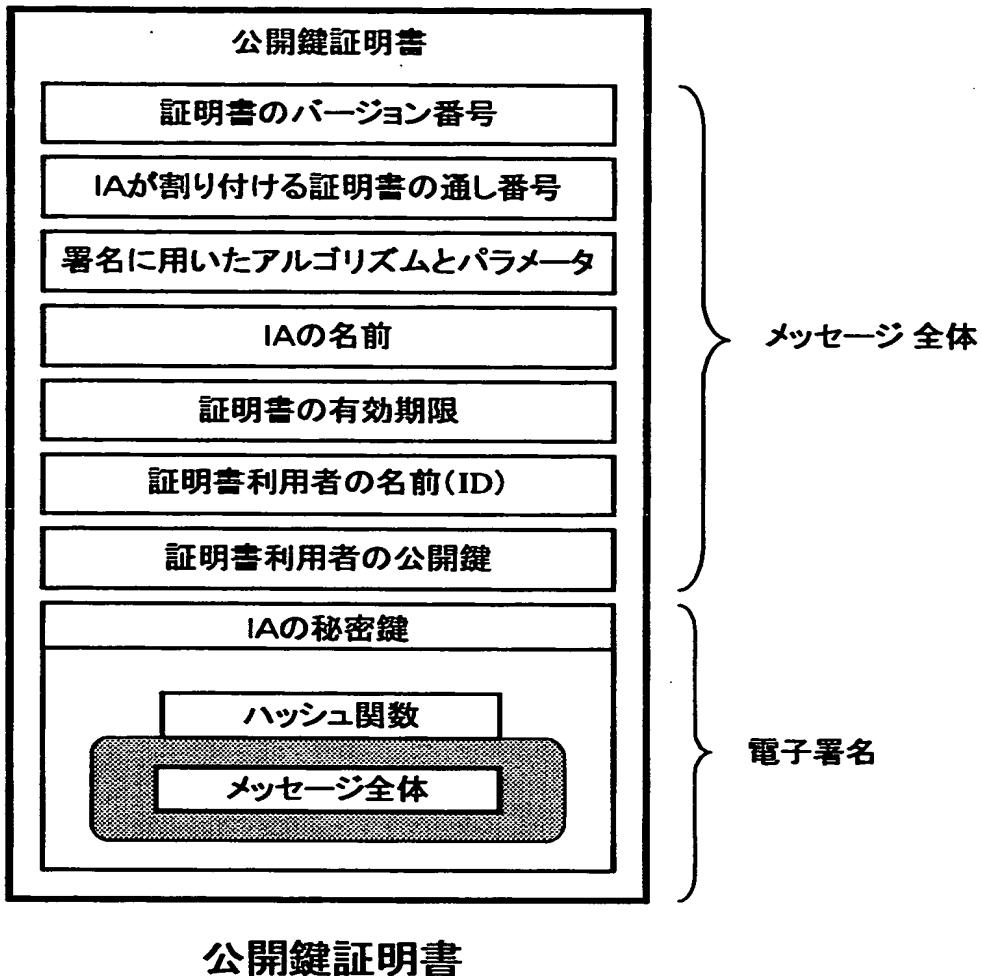
【図3】



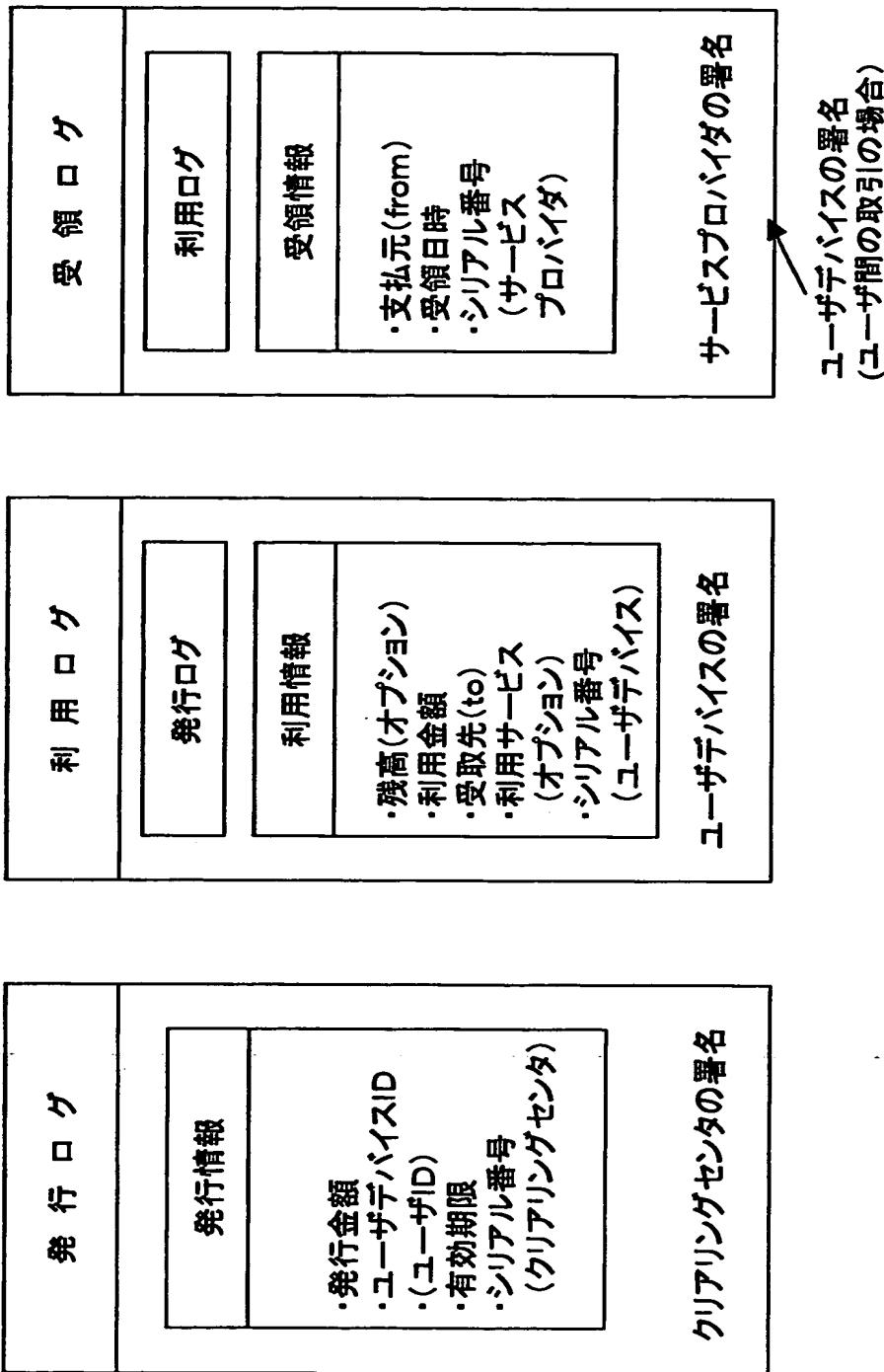
【図4】



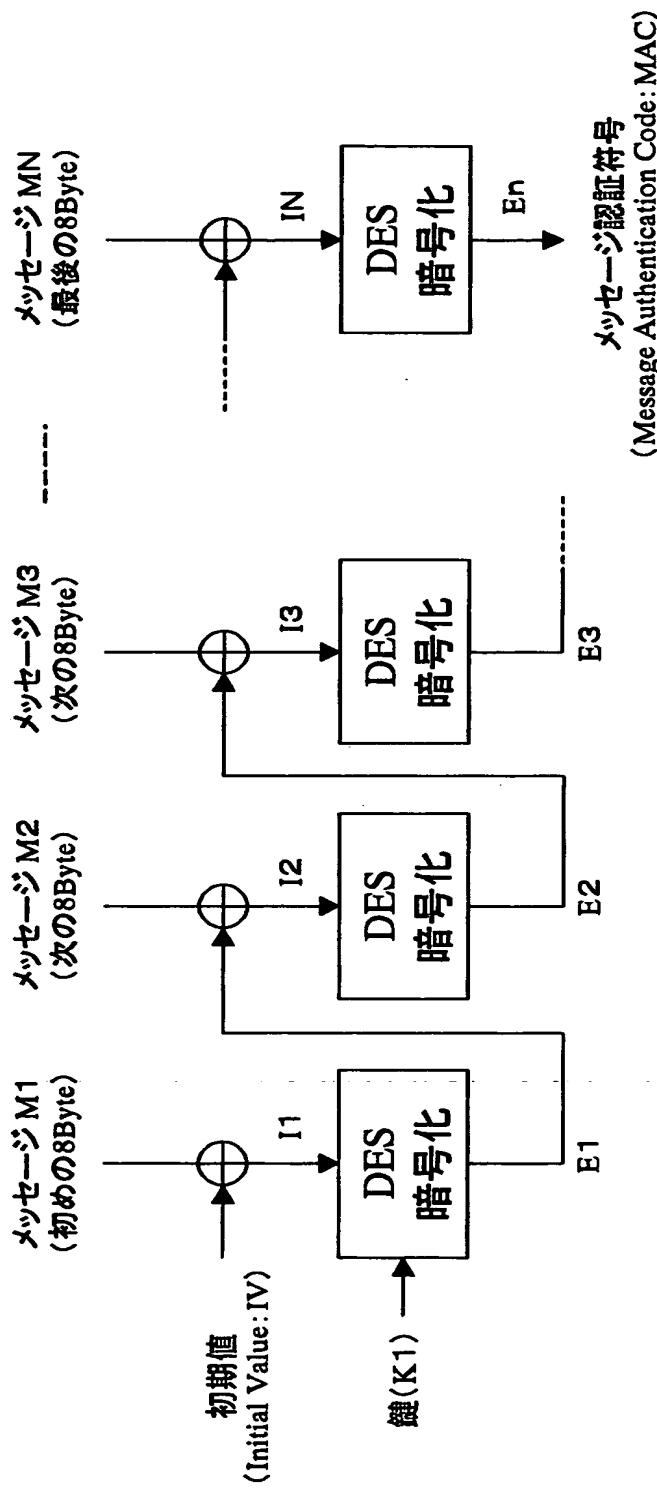
【図5】



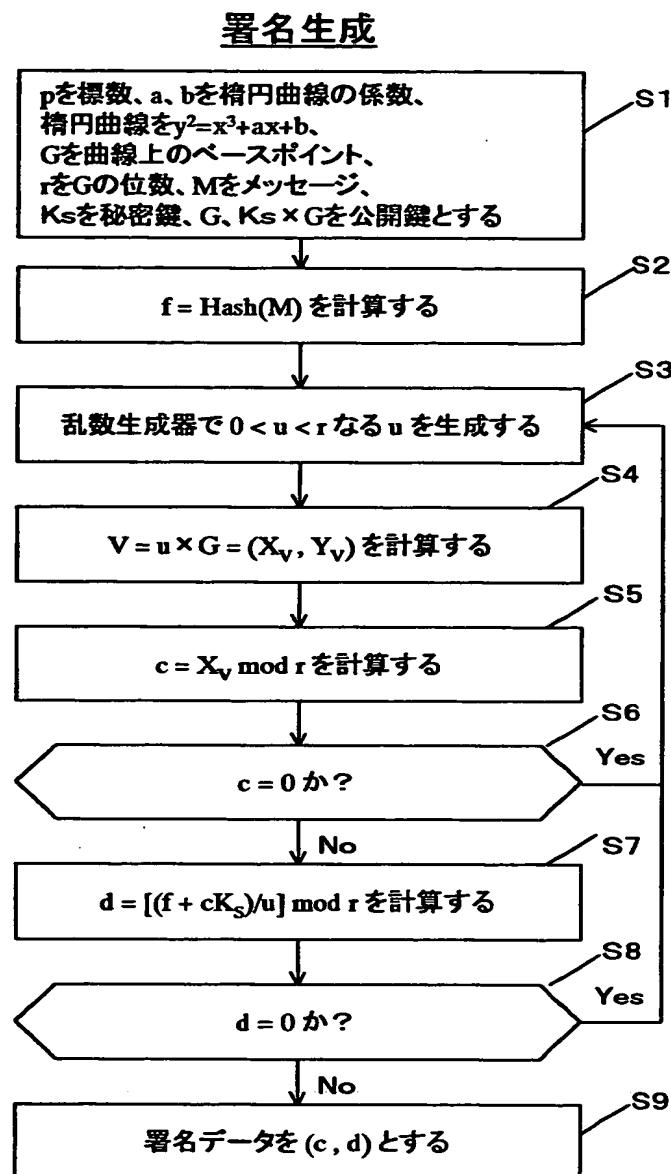
【図6】



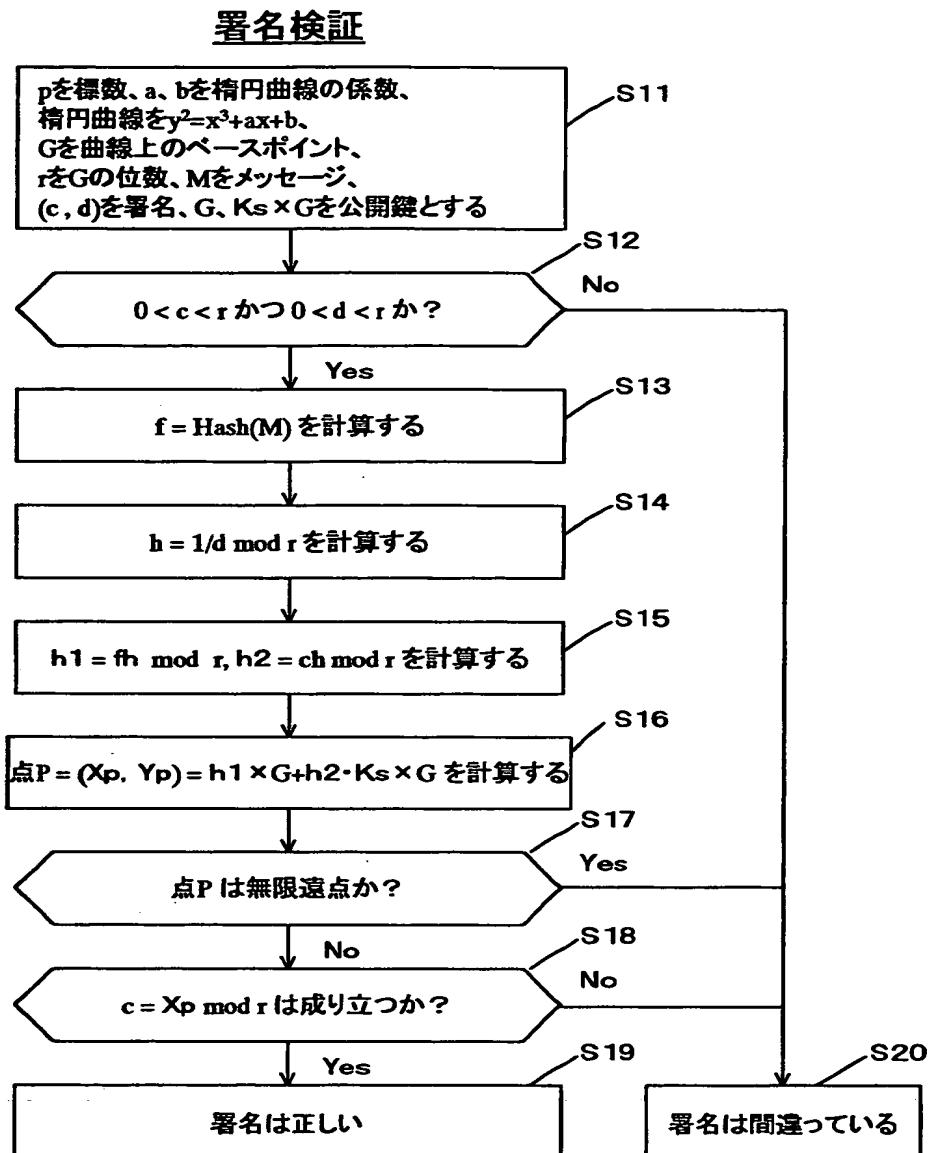
【図7】



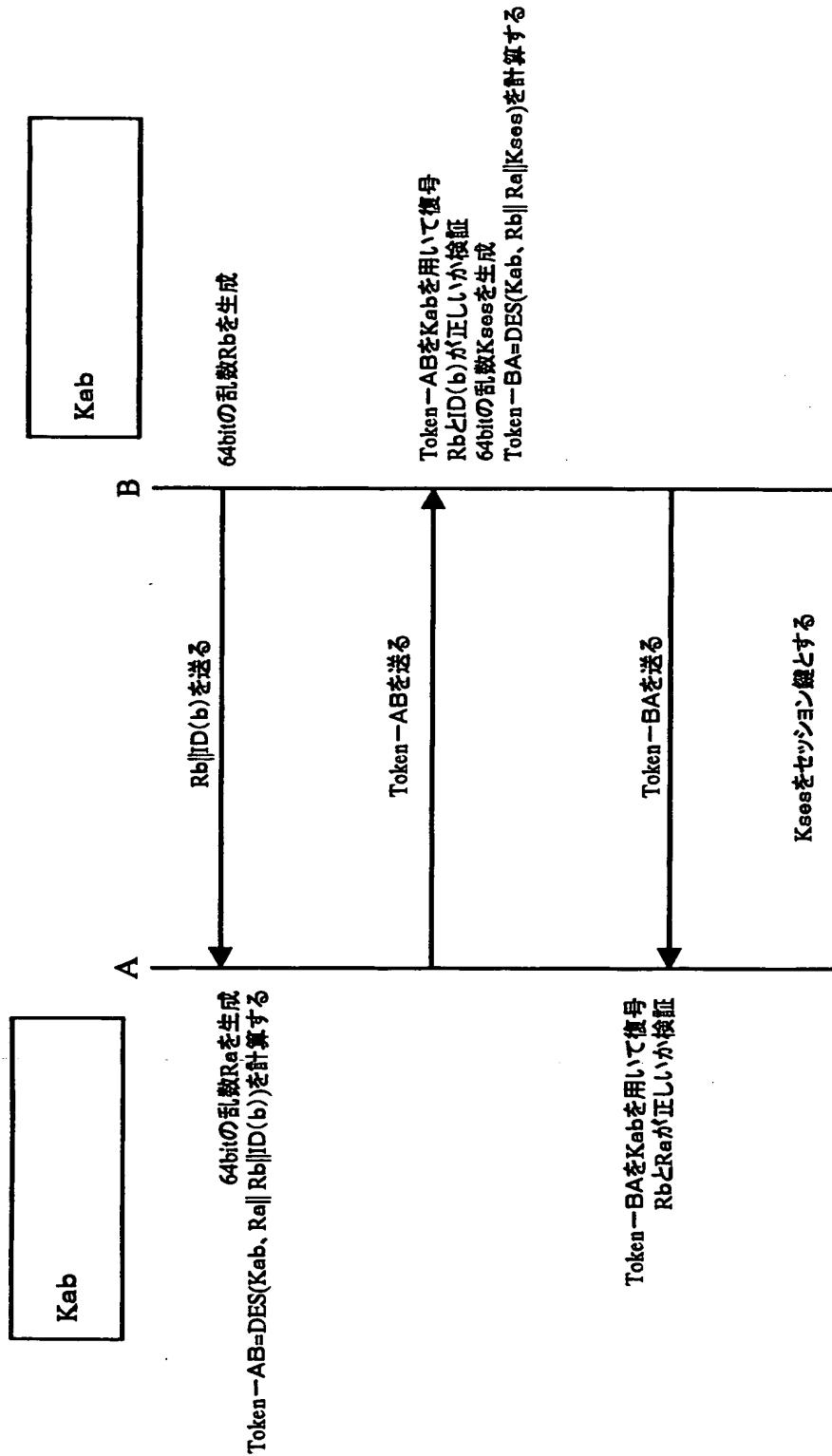
【図8】

署名生成(IEEE P1363/D3)

【図9】

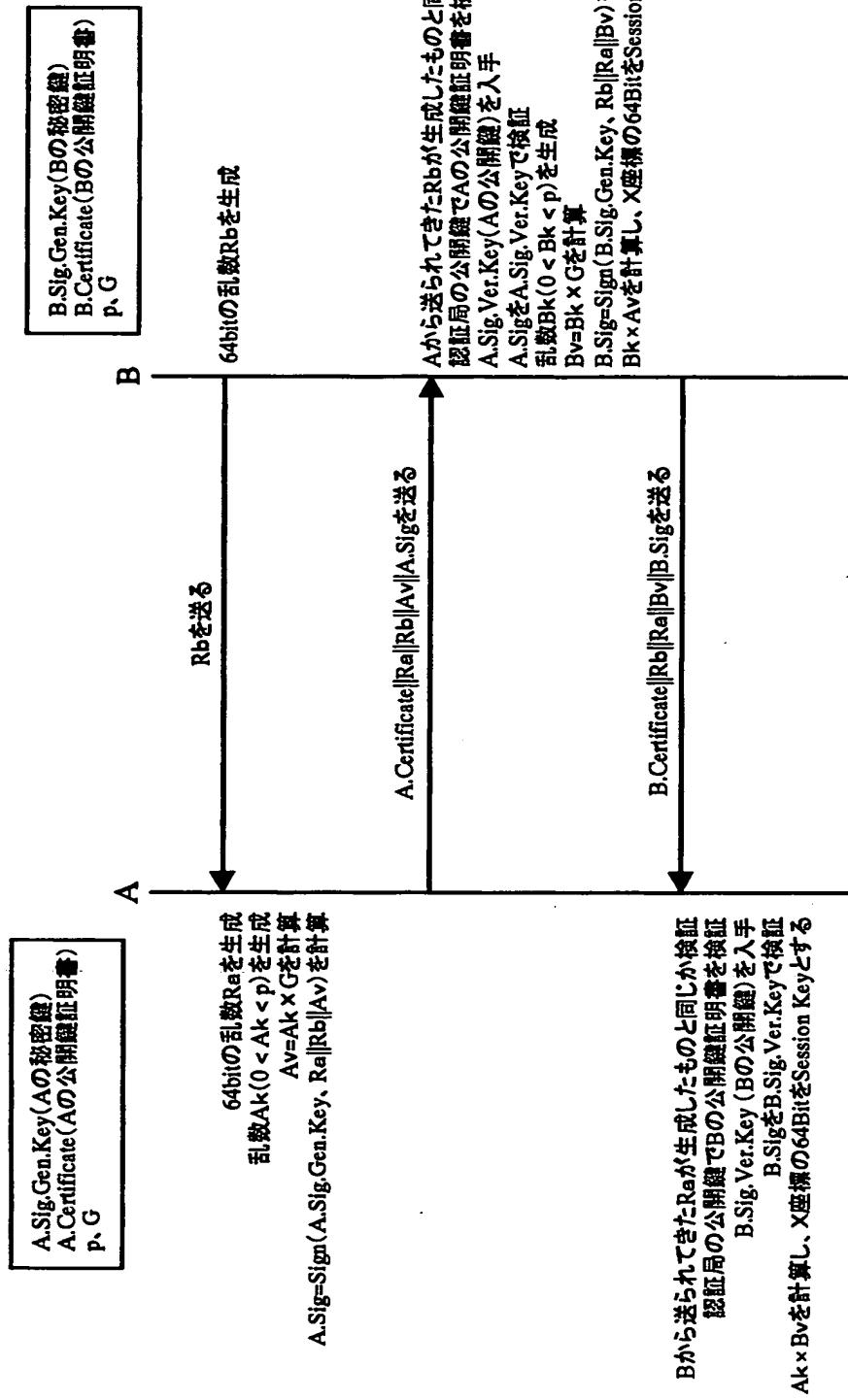
署名検証(IEEE P1363/D3)

【図10】



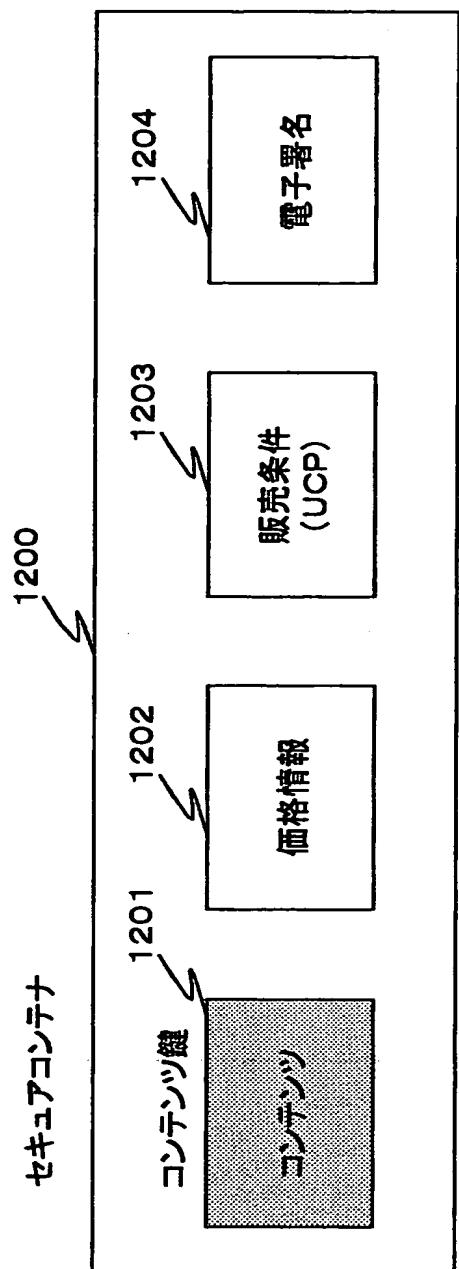
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図11】



ISO/IEC 9798-3 非対称鍵暗号技術を用いた相互認証および鍵共有方式

【図12】



【図13】

1301	データの種別
	取扱方針の種類
	取扱方針の有効期限
	コンテンツID
	コンテンツプロバイダID
	取扱方針ID
	取扱方針バージョン
	地域コード
	使用可能機器条件
	使用可能ユーザ条件
	サービスプロバイダID
	UCP世代管理情報
	二次配信可能回数
	ルール数
	ルールアドレス
ルール1	ルール番号
	利用権タイプ
	利用権タイプ販売価格
	コンテンツ利益配分情報
	データサイズ
	:
ルールN	ルール番号
	利用権タイプ
	利用権タイプ販売価格
	コンテンツ利益配分情報
	データサイズ
	:
	(署名検証の有無)
	公開鍵証明書
	署名

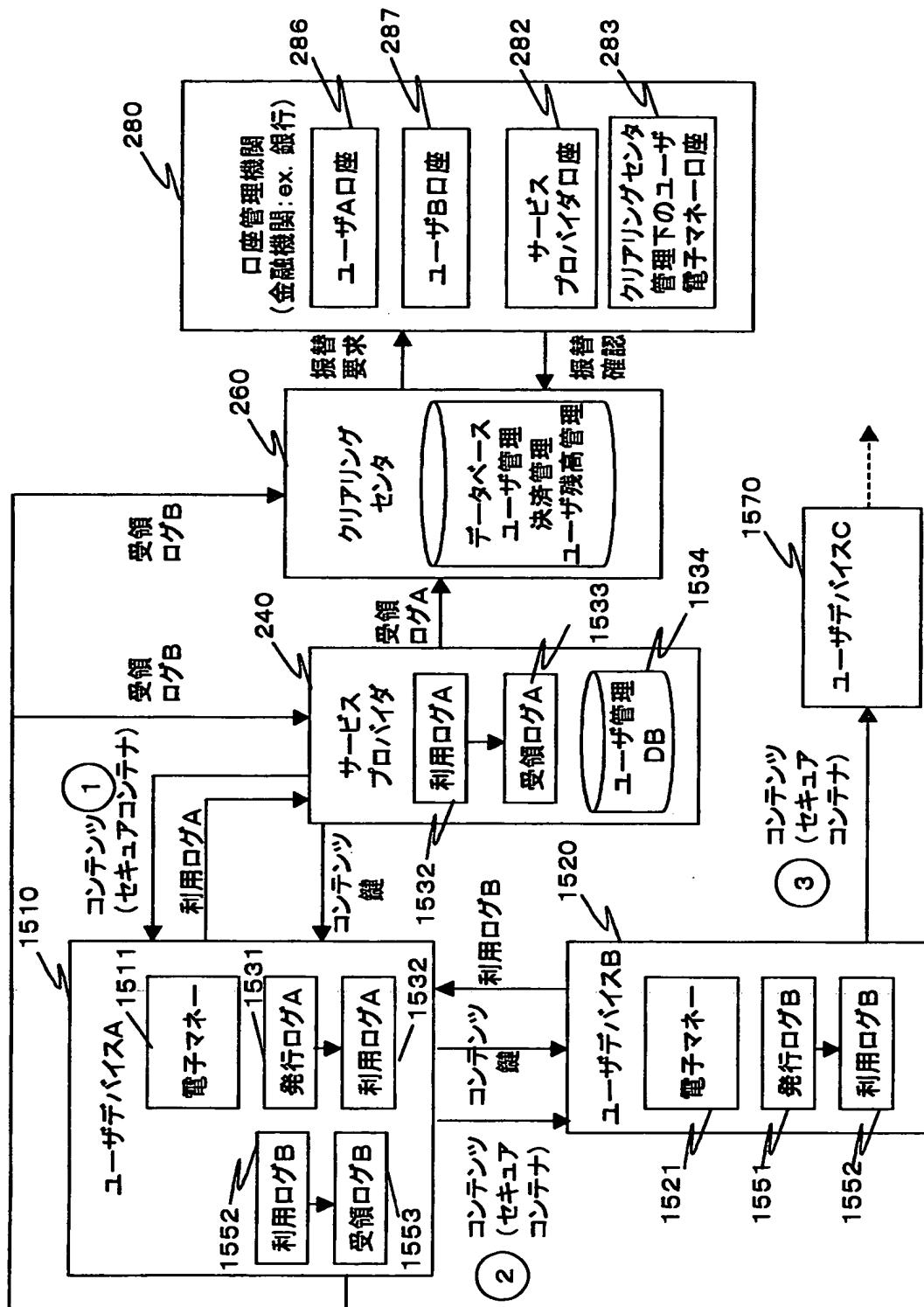
UCP(販売条件情報)

【図14】

データの種別	
価格情報の種類	
価格情報の有効期限	
コンテンツID	
サービスプロバイダID	
価格情報ID	
価格情報バージョン	
地域コード	
使用可能機器条件	
使用可能ユーザ条件	
コンテンツプロバイダID	
取扱方針ID	
ルール数	
ルールアドレス	
ル ル 1	ルール番号
	コンテンツ利益配分情報
	価格
	データサイズ
:	
:	
ル ル N	ルール番号
	コンテンツ利益配分情報
	価格
	データサイズ
:	
(署名検証の有無)	
公開鍵証明書	
署名	

価格情報

【図15】



【図16】

データの種別
使用許諾条件情報の種類
使用許諾条件情報の有効期限
コンテンツID
アルバムID
暗号処理部ID
ユーザID
コンテンツプロバイダID
取扱方針ID
取扱方針バージョン
サービスプロバイダID
価格情報ID
価格情報のバージョン
使用許諾条件情報のID
再生権(利用権)のルール番号
利用権内容番号
再生残り回数
再生権の有効期限
複製権(利用権)のルール番号
利用権内容番号
複製残り回数
UCS世代管理情報
UCS二次配信可能回数
再生権を保有する暗号処理部ID

1601

1602

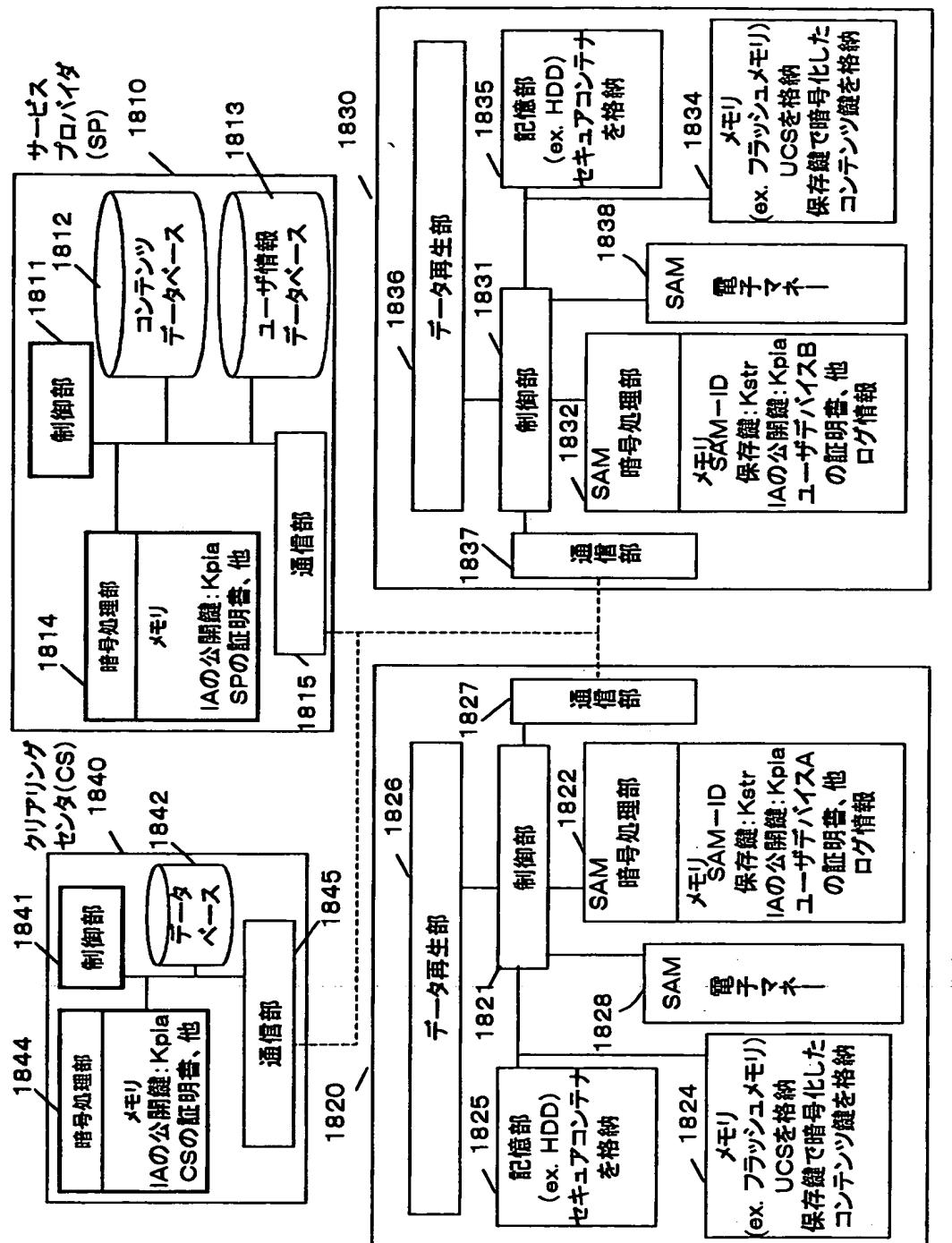
UCS(使用制御情報)

【図17】

データの種別	
1701	暗号処理部ID
	ユーザID(支払元)
	コンテンツID
	コンテンツプロバイダID
	取扱方針ID
	取扱方針バージョン
	サービスプロバイダID
	価格情報ID
	価格情報のバージョン
	使用許諾条件情報のID
	ルール番号
	コンテンツプロバイダの利益額／利益率
	サービスプロバイダの利益額／利益率
	その他関係者の利益額／利益率
	UCP世代管理情報
	コンテンツプロバイタの設定送信情報データサイズ
	コンテンツプロバイタの設定送信情報
	サービスプロバイタの設定送信情報データサイズ
	サービスプロバイタの設定送信情報
	受領日時
	シリアル番号
	供給元ID
1702	

受領情報

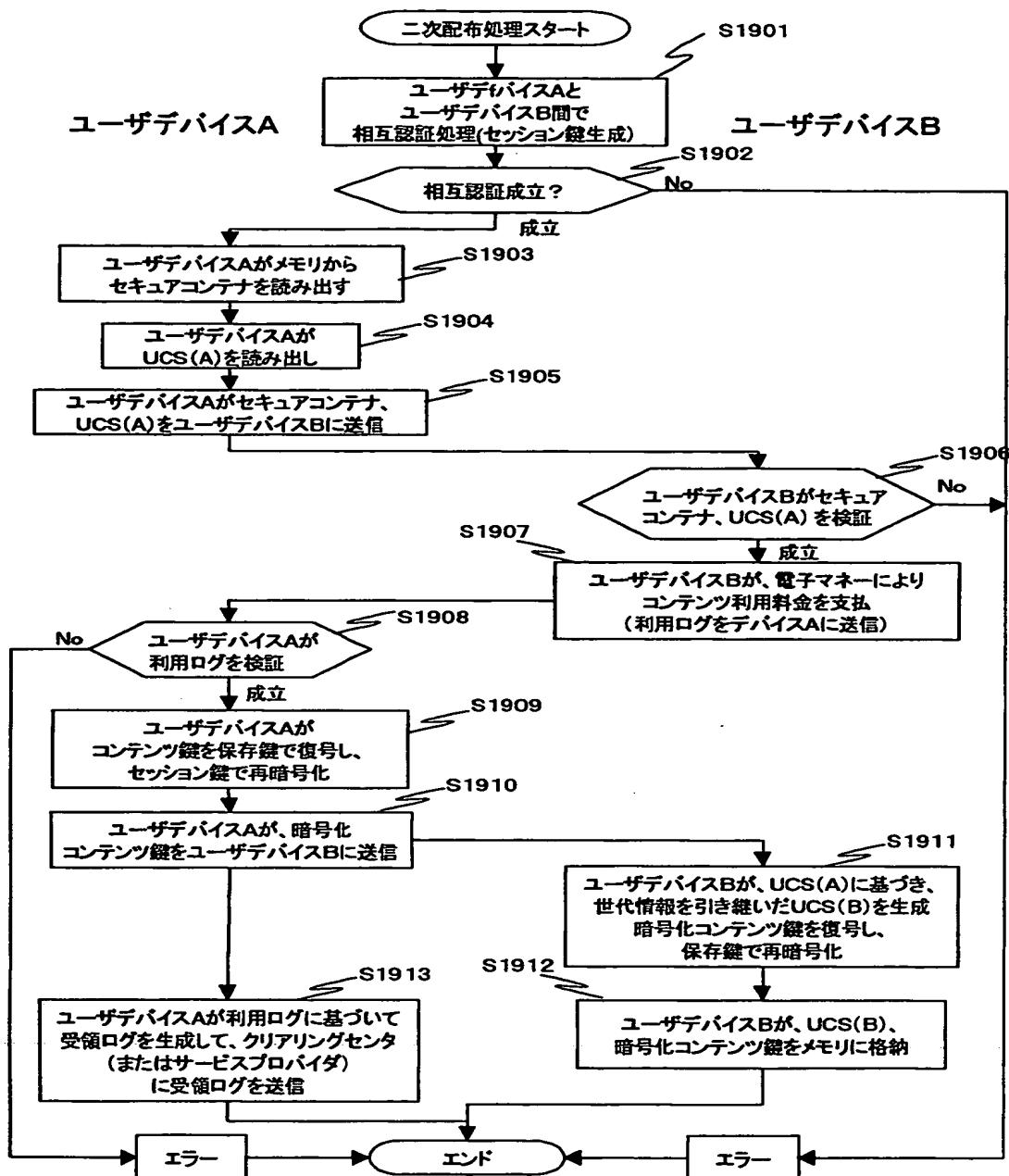
【図18】



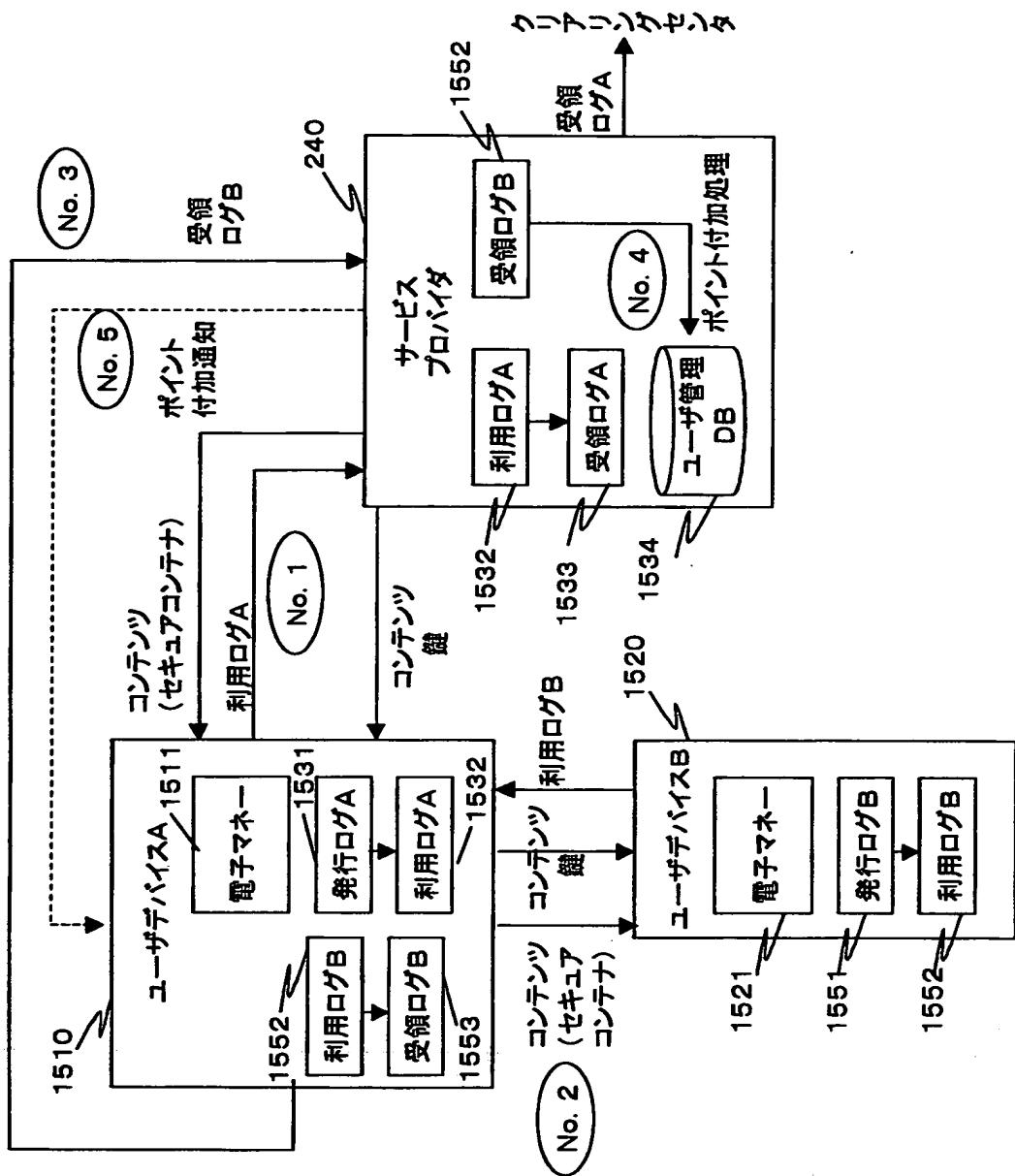
ユーザバイスA

ユーザバイスB

【図19】



【図20】

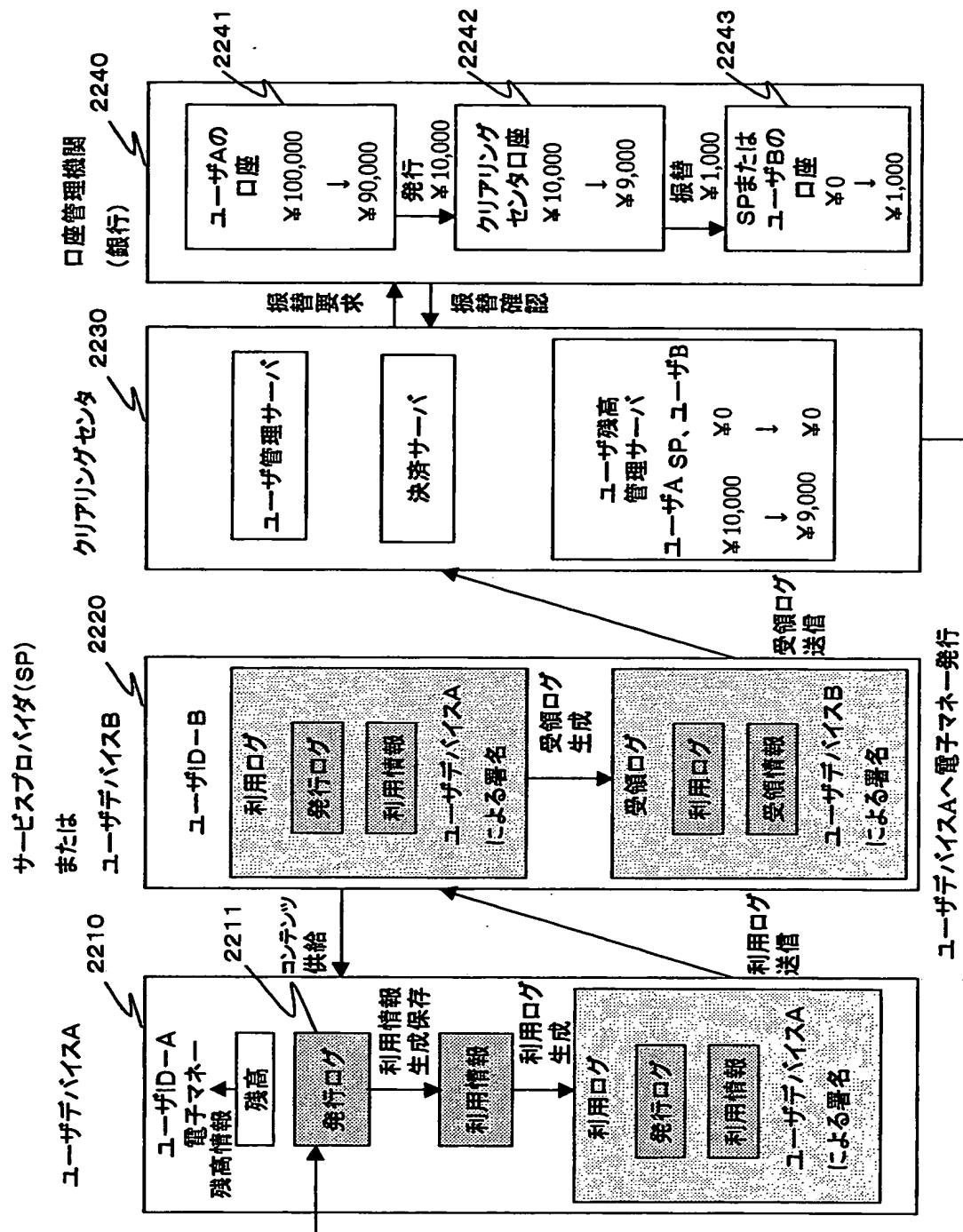


特2000-071103

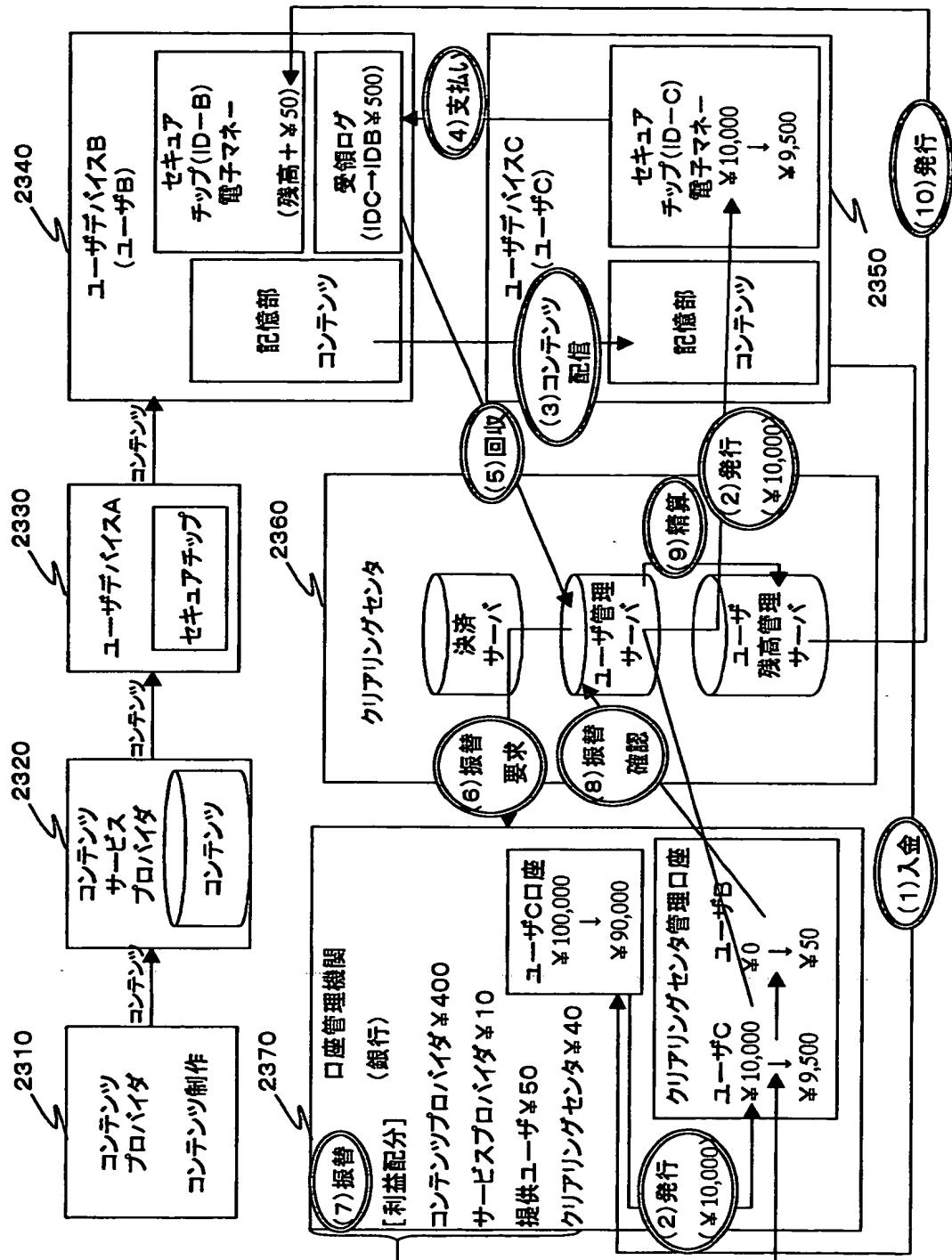
【図21】

ユーティリティID	ユーティリティバイスID	コンテンツID	受領ログID	ポイント
ABC0001	CDE00021	AAA001	BBB001	02
ABC0002	CDE00027	B05002	BA8822	05
ABC0003	CDE03211	CC0812	BA0214	12
:	:	:	:	:
BBC0231	EED02333	ABD325	BAA883	07

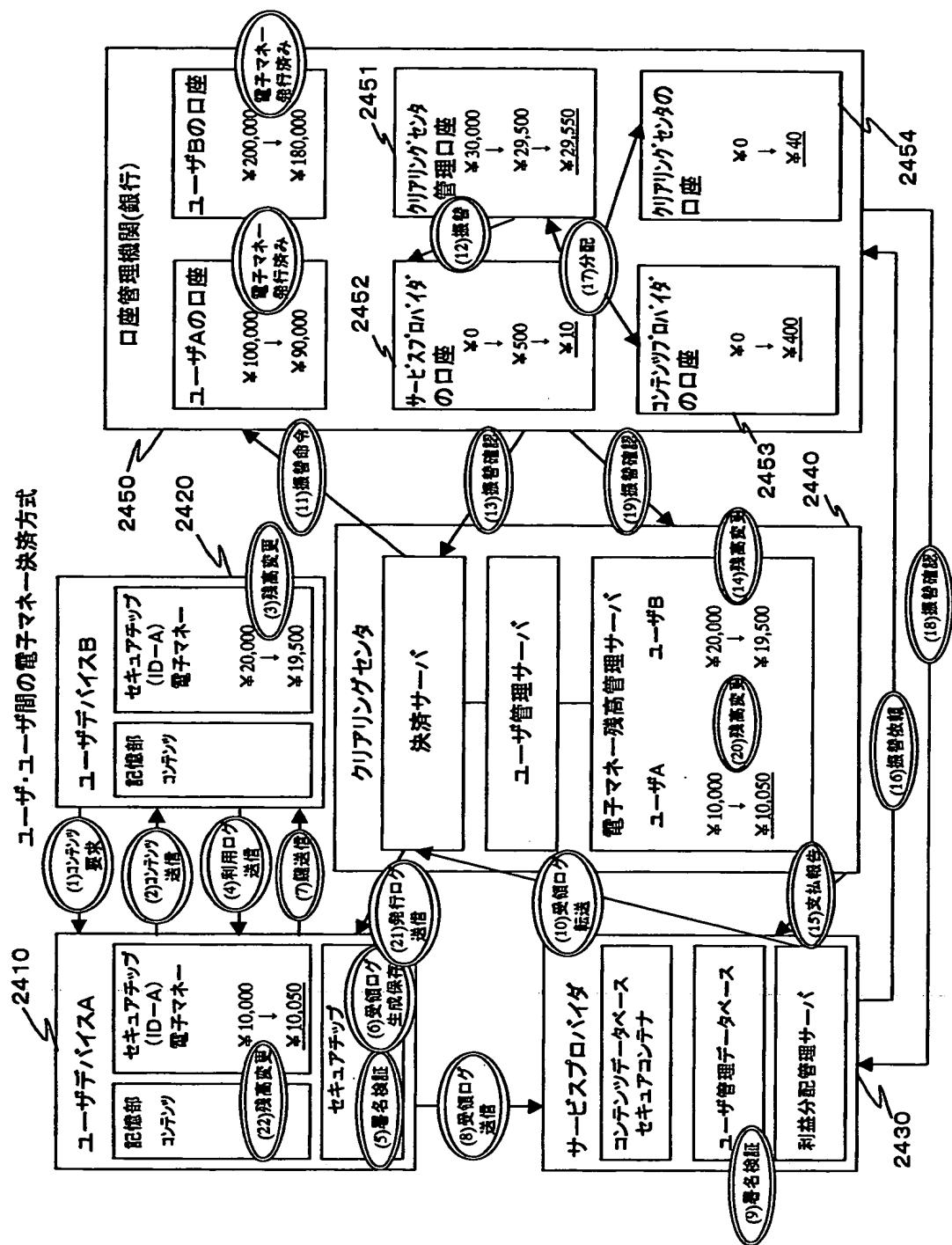
【図22】



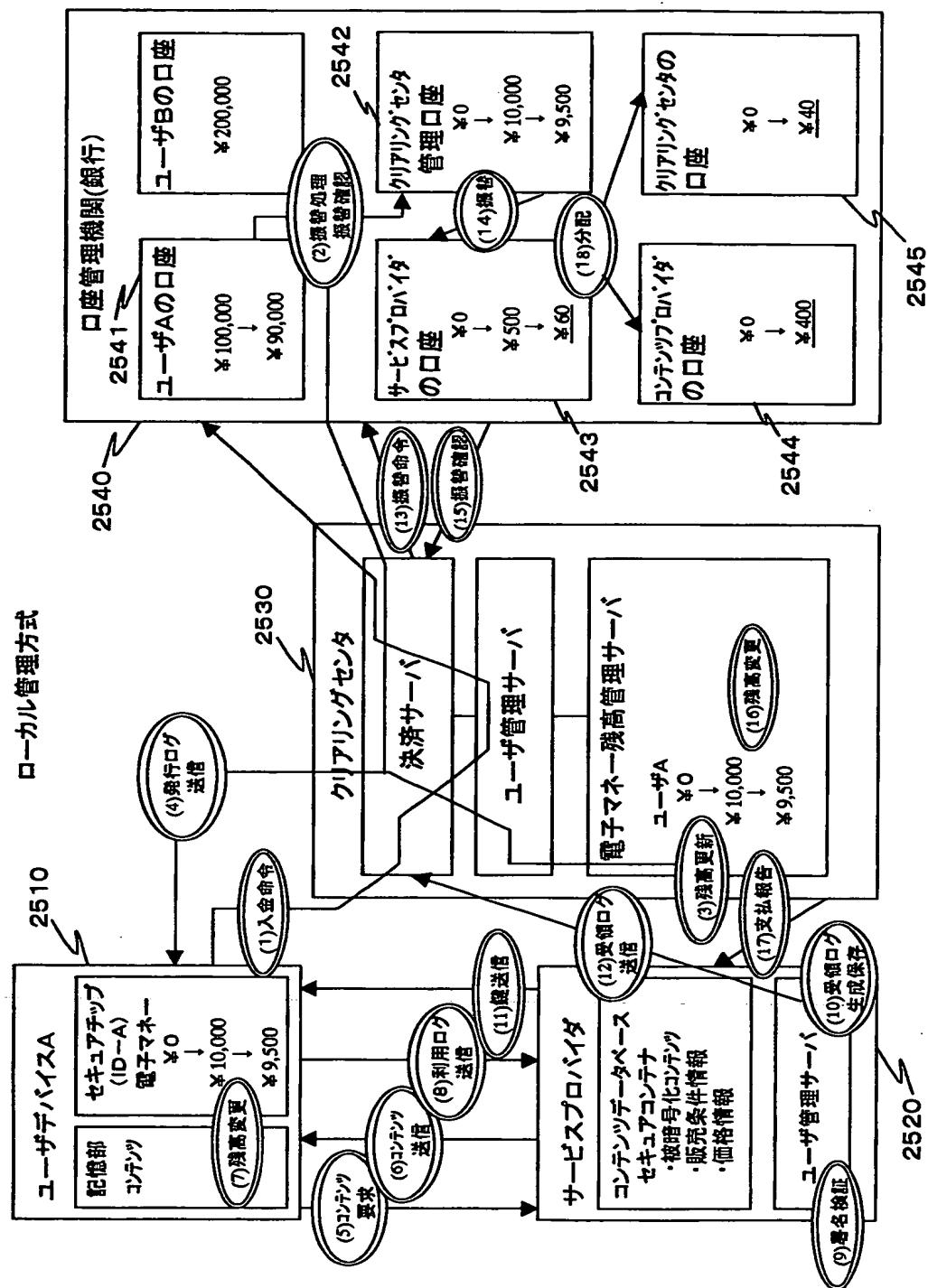
【図23】



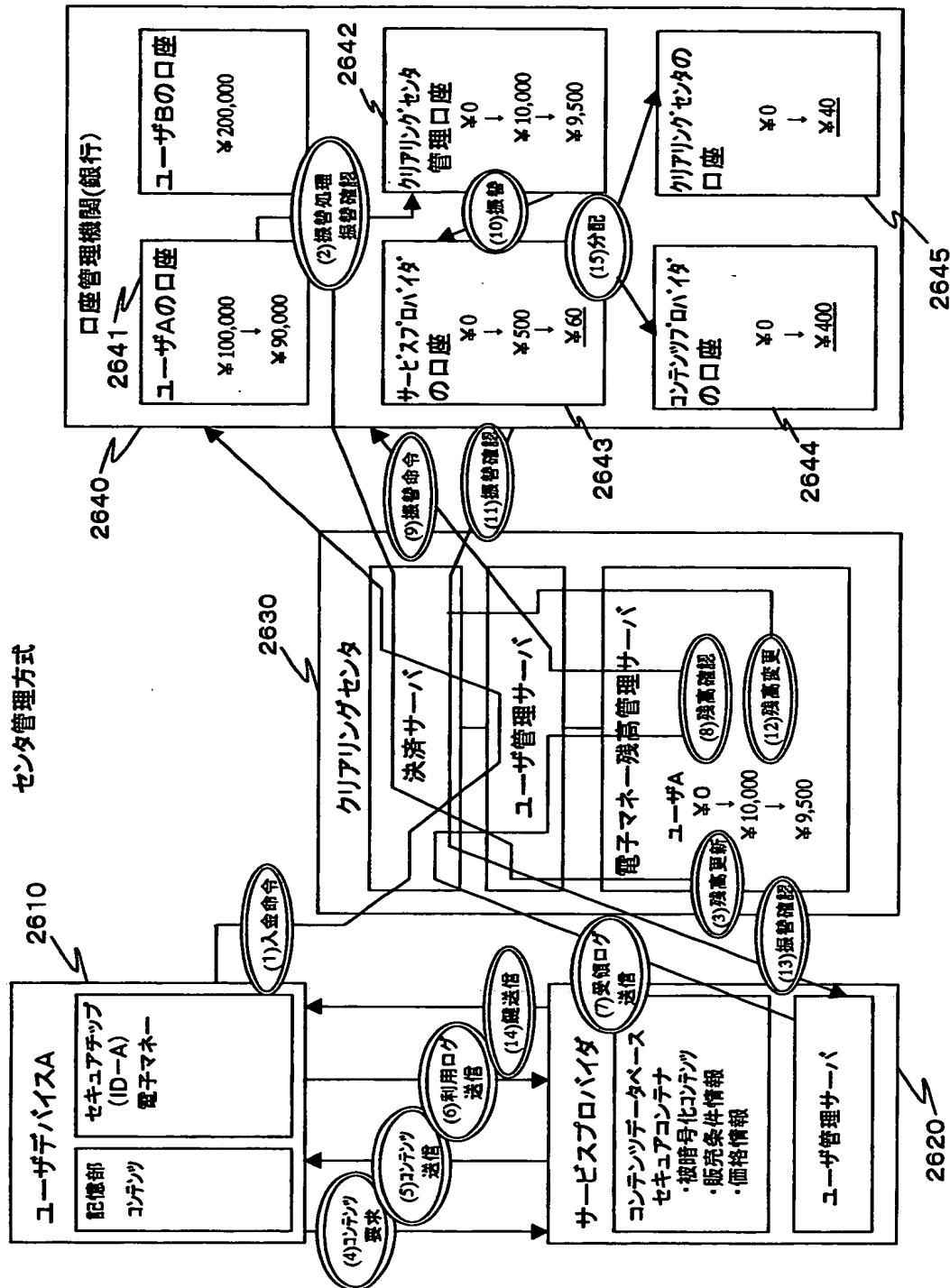
【図24】



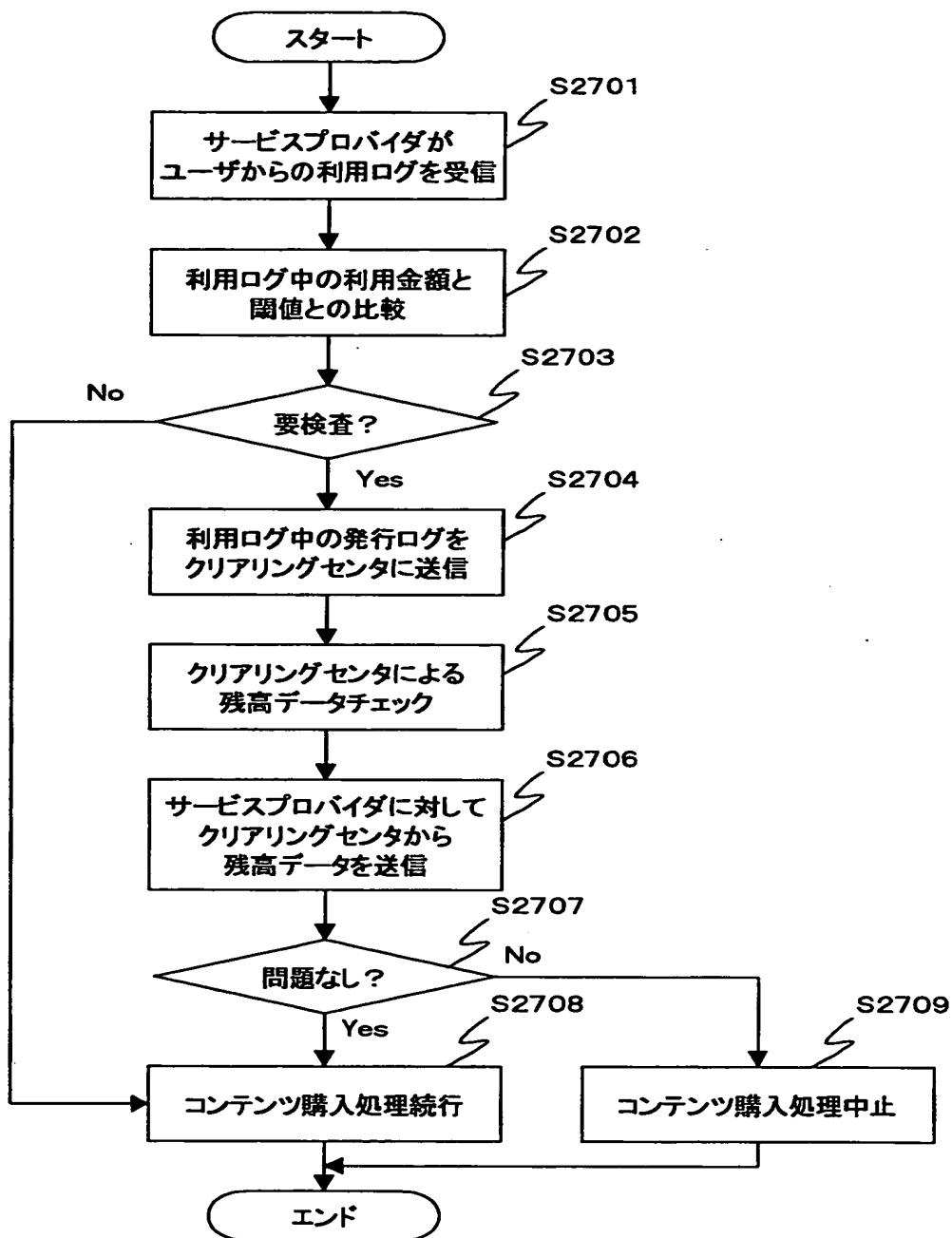
【図25】



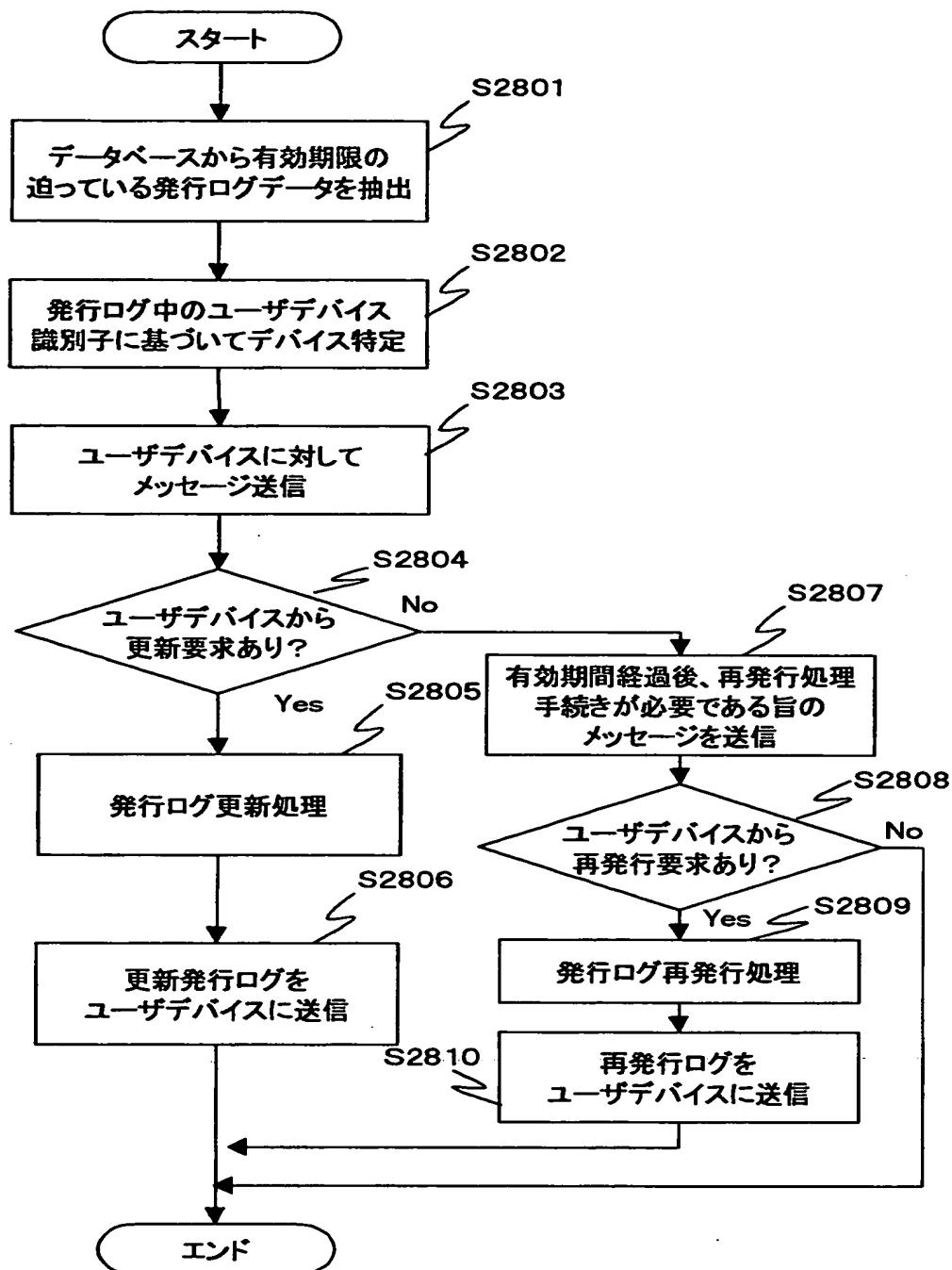
【図26】



【図27】



【図28】



【書類名】 要約書

【要約】

【課題】 コンテンツの二次配信の回数を制限可能としたコンテンツ二次配信制限システムおよびコンテンツ二次配信制限方法を提供する。

【解決手段】 コンテンツのユーザデバイス間での販売条件を設定した販売条件情報（UCP）を持つセキュアコンテナを構成した。UCPはユーザデバイス間の並列的なコンテンツ流通回数の上限情報としてUCP二次配信可能回数情報を持つ。コンテナを購入するユーザデバイスは、コンテンツ流通回数を設定したUCS二次配信可能回数情報を含む使用制御情報（UCS）を生成してメモリに格納する。コンテンツ二次配信時に、UCS二次配信可能回数情報の条件確認処理を実行して、条件範囲内であるときのみコンテンツ配信を可能として、流通回数が上限を超えた場合のコンテンツ配布を不可能とした。

【選択図】 図19

出願人履歴情報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日

[変更理由] 新規登録

住 所 東京都品川区北品川6丁目7番35号

氏 名 ソニー株式会社